



THE ARAB ORGANIZATION
FOR ADMINISTRATIVE DEVELOPMENT

ELECTRONIC GOVERNMENT

FOR THE 21ST CENTURY
A PRACTICE FIELD REVISITED

PROFESSOR ALI M. AL-KHOURI



**The Arab Organization for Administrative
Development Publications**

League of Arab States

Copyright © 2018 by The Arab Organization for Administrative Development. All rights reserved.

This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations used for the purpose of scholarly citation.

Printed in the Arab Republic of Egypt

ISBN 0-9000000-0-0

The Arab Organization for Administrative Development
P.O. Box 2692, New Cairo
Cairo, Arab Republic of Egypt

Tel: (202) 22580006

Fax: (202) 22580077

Email: arado@arado.org

www.arado.org

TABLE OF CONTENTS

Foreword	18
Introduction	22

1

E-Government Transformation - The Global Scenario	27
1.1 The Impact of Transformation On Governance	30
1.2 Going The Citizen-Centric Way: E-Government Transformation	32
1.3 Challenges in e-government Transformation	35
1.4 Stakeholder Perspectives	39
1.5 Striding Towards Alignment	41
1.6 Key Drivers and Enablers	42
1.7 Trust Establishment Around The Globe	44
1.8 Conclusion	46

2

Factors That Accelerate e-governance Transformation	49
--	-----------

2.1 E-Government Conceptual Model	51	3.2.5 Bahrain	94
2.2 E-Government Transformation	52	3.2.6 Canada	94
2.2.1 E-Government Transformation		3.2.7 The United Arab Emirates (UAE)	95
Management Framework	54	3.2.8 The USA	96
2.3 Push and Pull Factors	56	3.2.9 U.N. e-government Index	97
2.4 Benefits of Delivery and Incentives	58		
2.5 Out-Of-The Box E-service Innovation	59	3.3 Key Lessons Learned	100
2.6 Anywhere Anytime Access	66	3.4 TRANSFORM Strategy	107
2.7 Personalized Experience	71		
2.8 Blue Ocean Strategy for Value Innovation	73	3.4.1 Rocket Analogy To e-govt. Projects	107
2.9 E-Government Transformation Acceleration		3.4.2 The TRANSFORM Model	109
Framework	75	3.4.3 Stakeholders	111
2.10 Key Success Factors	79	3.4.4 Expectations	112
		3.4.5 Project Benefits	112
		3.4.6 Performance Indicators	113
		3.4.7 Enablers	113
		3.4.8 Resistance	114
		3.4.9 Thrust	119
		3.4.10 Navigation (Project Management)	123

3

An Integrated Transformation Strategy 83

3.1 Integrated Strategy For An Integrated Vision	84
3.2 Integrated Approach – Global Experiences	90
3.2.1 Germany	90
3.2.2 Belgium	91
3.2.3 Estonia	92
3.2.4 Singapore	93

3.5 Conclusion 124

4

Strategy Execution & Operational Models 127

4.1 Guiding Principles	128
4.2 Issues & Challenges	130
4.3 E-governance Transformation Contexts	132
4.3.1 G2C and B2C Context: Citizen Services	133
4.3.2 G2G and G2B Context: Integration & Interoperability	135
4.3.3 Enterprise Context: Security, Efficiency & Accountability	136
4.4 Towards Citizen Centric and Citizen Delight	138
4.5 Key Operational Aspects	140
4.5.1 Infrastructure	141
4.5.2 Policy	142
4.5.3 Governance	143
4.5.4 Outreach	144
4.6 The Role Of Federal Enterprise Architecture	146
4.7 Realization Roadmap	149
4.8 Governing e-governance Transformation	153
4.8.1 Service Governance Framework	155
4.9 Embracing Mobile Technologies In Transformation	159
4.10 Key Success Factors	162
4.10.1 Information And Data Strategies	162

4.10.2 Information Technology Strategies	163
4.10.3 Organizational & Managerial Strategies	164
4.10.4 Legal And Regulatory Strategies	164
4.10.5 Institutional and Environmental Strategies	165
4.11 Conclusion	165

5

Agencies and Departments	169
5.1 Issues and Challenges in bringing Transformation to the Agencies	171
5.2 Importance of an Agency Enterprise Architecture Strategy Aligned with Federal Enterprise Architecture	172
5.3 Role of Interoperability Standards & Frameworks	175
5.4 Metrics & Measurement for Agency Level Transformation	182
5.5 Supervision and Compliance	188
5.6 Conclusion	191

6

National Identity Management Systems: Building Trust in e-government	193
6.1 Last Mile Challenges in E-Service Delivery	196
6.2 Trust Enhancing Technologies	199
6.3 A System for National Identity Assurance	203
6.4 E-Identity as a Key Enabler in E-Governance	208
6.5 Important E-Identity Services that Accelerate e-Governance Transformation	212
6.6 GCC National Identity Management Systems – A Case Study	215
6.7 Role of Post-issuance Identity Adoption Standards & Technologies	221
6.8 The Last Mile Enabler for e-Governance Transformation in GCC Countries	222
6.8.1 Streamlining the Integration	225
6.9 GCC Identity Systems Interoperability Model Interoperability Model	228
6.10 M-Government and Mobile Identity	231
6.11 Value Innovation Strategy Around Smart Identity Systems	233

6.11.1 Stages of CIVIC IDEA Realisation	234
6.11.2 Dimensions of the CIVIC IDEA	237
6.12 Conclusion	239

7

Epilogue	241
Bibliography	251
Acronyms	263

LIST OF TABLES

Table 1:	Challenges Associated with the Four Stages of the Development E-Government Services.	38
Table 2:	Key Activities for E-Government Realization.	151
Table 3:	Key e-Identity Services to Enable and Accelerate e-governance Transformation.	214
Table 4:	Strategic Objectives of Identity Management Systems in GCC Countries.	216

LIST OF FIGURES

Figure 1:	Key Transformational Trends	28	Figure 22:	Card Holder Roles	218
Figure 2:	Pillars of E-Government Transformation	34	Figure 23:	Complexity of Identity Systems Integration	224
Figure 3:	E-Government Conceptual Model	36	Figure 24:	Solution for Streamlining Enterprise Identity Integration	226
Figure 4:	Government, Business and Citizens Perspectives of E-Government Transformation	40	Figure 25:	Conceptual Model for e-Identity Adoption	230
Figure 5:	E-Government Conceptual Model	50	Figure 26:	UAE Mobile Identity Strategy	232
Figure 6:	E-Government Transformation Management Framework	55	Figure 27:	Stages of CIVIC IDEA Realization	234
Figure 7:	EERC Grid of E-Government	72	Figure 28:	Growth Distribution across CIVIC IDEA Phases	236
Figure 8:	E-Government Acceleration Management Framework	76	Figure 29:	Dimensions of CIVIC IDEA	238
Figure 9:	Rocket Analogy	108	Figure 30:	E-Government Transformation Model	243
Figure 10:	TRANSFORM Model	110	Figure 31:	Augmented Identity	246
Figure 11:	E-Government Transformation Context	134	Figure 32:	Conventional Transformation vs. Accelerated Transformation	247
Figure 12:	Enterprise Logical Access Control Systems	137			
Figure 13:	Enterprise Physical Access Control Systems	137			
Figure 14:	Enterprise Architecture Maturity Level Comparison	148			
Figure 15:	E-Government Transformation Management Governance Framework	155			
Figure 16:	Enterprise Architecture Strategy	174			
Figure 17:	Technology Stack for System Interoperability	183			
Figure 18:	Steps of E-Government Performance Monitoring	189			
Figure 19:	E-Government Citizen Interaction	197			
Figure 20:	Credential Lifecycle	206			
Figure 21:	The GCC Smart Identity Systems Capabilities	217			

FOREWORD

Around the world, the future of the mechanism of government is being more and more scrutinized and discussed so a continual re-evaluation is occurring regarding the transforming role of governance at a time in this 21st century when the world itself is undergoing rapid and dramatic technological changes. Efforts are underway the world over for e-government services to be made available ubiquitously for the population. A country must, therefore, understand its citizens and their needs well, as an e-citizen-centric government is aimed towards every citizen in every community having access to all forms of e-government at the federal, provincial and local levels.

The demand to transform a government from its traditional agency role and a department-centric model to a 'citizen-centric' and 'always available' model is growing steadily across the globe. It is widely expected that this transformation will enhance citizens' quality of life in terms of greater convenience when availing themselves of government services, which will result in increased citizen satisfaction levels.

E-government is now a well-established paradigm, and is already a generation old; yet, not all governments are fully aligned with this new e-path. Both citizens and governments, including all intermediaries and enablers, service providers and government departments, now interact on a virtual, integrated platform. Thus, it is no longer viable for a government to be still in project-mode or to be focused on mere electronic initiatives for specific government-citizen services in an ad-hoc or independent manner.

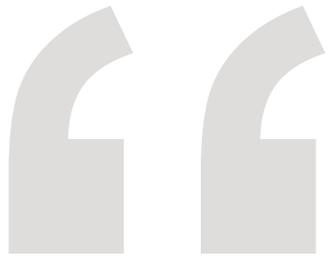
E-government calls for the seamless collaboration of government departments, partners, other stakeholders and citizens with the integrated use of Information and Communications Technologies (ICTs), which are critical to achieving the desired transformation. This new approach stems from the discovery that the traditional approach of fragmented e-government initiatives has actually failed to meet the increasing demands of citizens.

This is the future of governments; fully digital. Any realization strategies and plans for creating such future governments must not only involve themselves with, but also take advantage of all new innovative technologies in the areas of security and mobile services, coupled with the adoption of advancements in the area of electronic transactions.

This can be construed as the beginning of a new era in the area of the convergence of e-government and electronic identity adoption strategies. Smart government is all about availability, convenience and security. Therefore, government services are being deployed on smart phones for ease of access and 24-hour availability while the identity management systems accord the protection and privacy of a user's identity enabling secure service delivery transactions.

The future will transform all existing e-government initiatives in an integrated manner, and fuse this transformation and transformed smart government to create a new unique digital eco-system for governance. This will only be done through comprehensive research and development combined with an innovation-driven, sustained value creation in an integrated manner.

This book has been written, therefore, not only for the professional or for the practitioner, but also for the citizen who is circumnavigating that road to dealing with e-governance. The book defines, explains, showcases and seeks to serve as the primary reference on the strategic framework and execution methods for transforming e-governance to make it citizen-friendly, harness the digital platforms to enhance and catalyse this transformation, as well as lay the foundations for a fully integrated and inclusive government for the empowerment of its citizens. This text will, thus, indeed serve well to augment and accelerate e-government adoption programs around the world.



H.E. Ambassador

Mohamed Mohamed Al Rabei

Secretary General,

Council of Arab Economic Unity

League of Arab States

INTRODUCTION

A full service e-government goes far to make communication between citizens, businesses and the government more transparent, and opens up new possibilities for the way in which information is presented and accessed. Of course, in this scenario, secure communication and the confidential handling of transactions of personal data have top priority. Thus, an e-government must do more than just improve services, save costs, make work processes more efficient, and enable independent work. A transformed e-government must offer more opportunities for its citizens to participate and have a voice in community matters.

E-government has two major components: the 'e' part which concerns technology management and the 'government' part which involves connected e-government - these converge to provide a seamless access experience for the citizen. Both parts together enhance the overall quality for a population that must access government services. In any scenario leading to e-government, the technology is the first to be managed along with the governance needs. The major factor that, of necessity, can bring about this unification and the much sought after seamless e-experience is a uniform citizen identity or a national identity program. An e-government project is an ecosystem of resources, processes and technologies. These three components work in close coordination in the implementation of any projects.

Even though technology is becoming more unobtrusive and seamless so that it is almost 'hidden' from users; it is technology-

dominant. Those who are computer-literate have definitely found that browsing is becoming more 'seamless' or 'transparent'; however, there are still many who do not have computers and some who do not even have cell phones. This means that computing really only serves those people who use computers. In a ubiquitous anywhere anytime government, technology serves 'as a means to an end' and, therefore, has to 'take a back seat to allow users to fully concentrate on 'the task at hand'. The provision of public services, on the other hand, is citizen-centric and governments cannot choose their customers and how they need to be served. Governments have the bigger responsibility of serving all citizens-- computer literate or not. As a result, governments must meet this 'digital divide' challenge.

Central to any e-government program is the citizen, thus a national identity card of some type is necessitated, which provides a unique identity for the individual. When this identity is provided as a digital identity profile, a person has not only the ability to transact in the digital medium, but should also have a common identification tool that can be used across all government departments. This is the unification factor that ensures the use of the same primary key across all government databases; therefore, enabling a seamless experience to the citizen across the government.

The different dimensions of e-government projects are quite complex. This makes the importance of having an effective and active overseer - for monitoring and evaluation, non-negotiable. In order to have a highly affective e-government, a framework such as this must be put in place to measure the output, outcome and overall impact to provide the required information for informed decision making,

with regard to implementing e-Services.

The GCC countries that now lead the world in many aspects (from economy, energy, oil, infrastructure, social empowerment, welfare, development, and urbanization) are now on the verge of embarking on a dynamic new e-journey to establish one of the most evolved Smart government frameworks. This integrates and once again transforms all the current e-governance Initiatives that leverage the national identity-based eco-system and the enabling platform. The GCC are thus in the process of creating a new form of opportunities – with secure smart identity systems and personal identity credentials transform the landscape of economic activity.

What is going on? These countries are paving the way to the early stages of what is now known as mobile (m)-government. Mobile devices are primarily designed as communication devices. Certain features and functions, less common or impossible under the e-government paradigm, such as the ability to contact government offices directly from the phone, or to receive automated text messages about news or emergency information are now included in the early stages of m-Government. As m-Government advances, more advanced functionality is being added including the possibility of e-voting and online poll participation, and due to the dispersed nature of mobile technology, higher usage numbers are expected than the similar functionality that was available only from traditional PCs.

This book will now take the reader e-step by e-step beyond the now of

e-government to the innovative design of the timely m-government as will be outlined here in the dynamic use of it in the GCC countries.

let's begin!

1

E-GOVERNMENT TRANSFORMATION

FROM

SYSTEMS
TECHNICAL ISSUES



TO

CAPABILITIES
BUSINESS
IMPACT

1. E-GOVERNMENT TRANSFORMATION THE GLOBAL SCENARIO

Today, economic and political systems are under tremendous stress, worldwide. Systemic, financial and governance failure continues to be a great risk to government operations in the foreseeable future. This aspect is testing the resilience of nations across the world. Global growth projections continue to be low as major economic powers are finding it difficult to emerge from the impact of the economic meltdown. There is increasing concern as well regarding the socio-political conditions that have resulted from the increased burden on the public.

As of mid-2013, the Middle East and the GCC continue to witness widespread social unrest. People are increasingly concerned about the health of banking and public service delivery systems amidst the stagnant economic growth. The competitiveness of the region grossly lags behind, especially, in the areas with respect to innovation, labour market efficiency, financial market development and market size. This is making countries in this region realise that collaborative gains must be achieved through shared infrastructure, more efficient and transparent institutions, and educational systems that are attuned to the changing needs of society. Some of the key transformational trends are the shifts from addressing systems and technical issues to building capabilities and business impact.

Figure 1: Key Transformational Trends

Specifically in the Middle East, countries face an issue of a low latent skill base by world standards that has resulted from relatively little research, development and innovation being prevalent in the region. These factors pose constraints on these countries' attempts to diversify from oil reserves to the knowledge and service sectors. The wealth generated through the energy reserves has to be put to use to ensure that the region's economies shift steadily to sustainable prosperity in order to become innovation based economies. To ensure success on this path, many reforms have been undertaken to improve the efficiency and openness of government and business systems. When these reforms start to yield results, they will push the region to an increasingly important position on the international scene.

1.1 The Impact of Transformation on Governance

For these reforms to be sustained, it is imperative that the associated e-governance systems and processes are made more efficient and transparent as well. Furthermore, in the fast changing world scenario, a nation's top leadership needs to have information at their fingertips, which would enable faster and informed decision making. This brings to the fore the adoption of Business Intelligence (BI) systems and customer behaviour analysis which would facilitate government decision making as well as contribute to continuous systems improvement.

At the operational level, as the stress on the financial systems continues, governments need to focus on delivering more to their public with less cost. This necessitates the elimination of redundant systems and processes across various government departments thus enabling interdepartmental integration. A key benefit of this approach is that it would break down departmental boundaries and project a single, unified government view. This would further contribute to the competitiveness of a country and lead to stronger investor confidence.

Traditionally, governments are found to be slow at adapting to new technologies. Considering the rapid pace at which new technologies are emerging, and the citizens' being willing to adopt newer platforms for increased convenience and mobility, there is a dire need for governments to switch to these newer technology platforms as well. This would allow governments to reach out to citizens through the medium of a citizen's choice on a case by case basis.

As governments strive to improve citizen services, various international ratings seek to track these reforms, thus providing pointers to the global ranking of a country based on various parameters. Lower rankings in these indices indicate reduced competitiveness of the country at the international level. In today's globalized competitive environment, it is imperative to top the charts.

1.2 Going the Citizen-Centric Way: E-Government Transformation

E-government models that have treated citizens as one undifferentiated mass have failed. On the other hand, revolutions in social networking have demonstrated how personalised solutions have worked. All these pointers converge at the key qualities a transformed government must strive for - personalized experience, global standards and localised responsiveness.

The traditional, department-centric view of public services is being rapidly replaced with a view of personalised experience and value co-creation. The current department-centric approaches of E-government today are neither adequate nor do they seem suitable for creating a personalized experience for citizens. Therefore, transformation is the need of the hour for E-government to become a platform for user centred experience (Pralhad and Krishnan 2008).

The much sought transformation is not without difficulties in how to adopt it and adapt it to the traditional government models which are merely transaction based. Currently, service access interactions by citizens at designated service delivery points are treated as discrete transactions. Models based on such discrete transactions limit the opportunity for value creation and a personalised experience. A suitable model in which citizens participate in value creation requires governments to move away from the transaction based approach to an on-going relationship with citizens. Such a model would enable the government to get detailed information on how individual citizens avail themselves of the services as well as a host of

other characteristics that can help in the continuous improvement of public service delivery. It is, therefore, imperative that the citizen or the customer of the public services participates in the value creation process.

This transformation is built on five pillars, as depicted in Figure 2.



Figure 2: Pillars of E-Government Transformation

Of course, transactions will continue to be an integral part of e-government. However, the value benchmarking is based on an ongoing citizen engagement that will result in the co-creation of value. Hence, the transformation to e-government is required in order for governments to evolve from a mere transaction relationship to a service relationship, and then go further to a superior personalised experience. Here, the value shifting is sought from the transaction itself (product) to a digital solution to the transaction experience.

1.3 Challenges in E-Government Transformation

Any e-government transformation touches every aspect of governance and, hence, it calls for a complete overhaul of a government’s strategy and systems. Just as the magnitude of benefits it accords to a country and its people is immense, so are the challenges it will face at each stage of the transformation in order to realize it. To understand this more and gain a better perspective, let’s consider a four stage transformation model that would lead to the delivery of e-government services depicted in Figure 3.

The first stage is service innovation, where governments identify the need for a specific service and engineer it to meet the specific requirements of all stakeholders. A key point to note here is that better service is the outcome of the service innovation process that stems from the needs of stakeholders. Hence, the primary objective of a service is to fulfill the associated needs of stakeholders in an efficient manner.

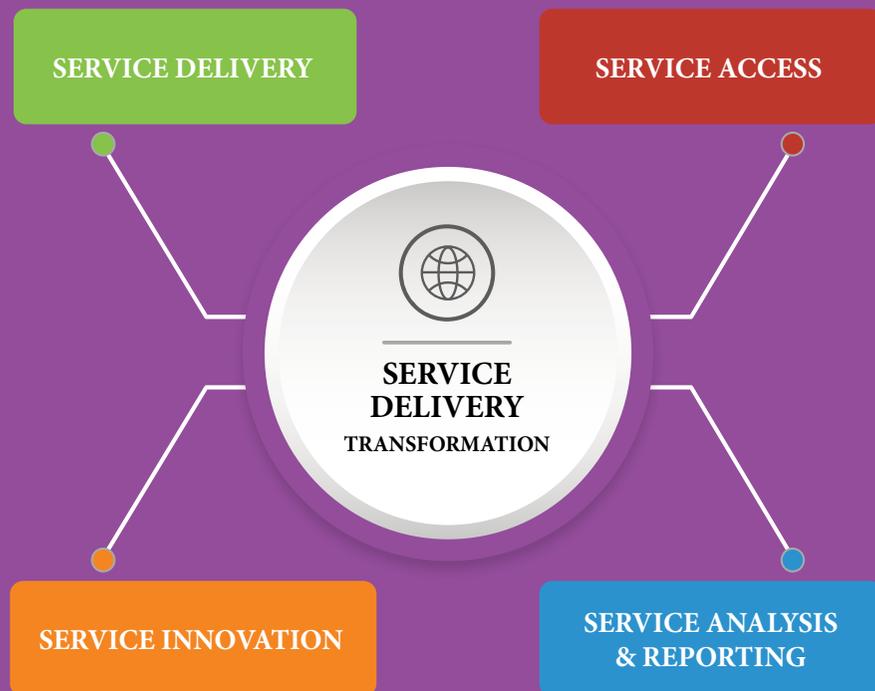


Figure 3: The Four Stages of Transformation to e-Government Service Delivery

Each service has a target population. Thus, service delivery aims to make a service accessible to the target population, considering the characteristics, capabilities and limitations of this group. Inclusiveness is one of the key values that service delivery should always be based on. Another aspect that governs service delivery is the Citizen Charter with Service Level Agreements (SLAs) that guarantee a level of service availability and the overall quality of the service experience to citizens.

The end objective of service is fulfilled when the target population avails itself of the service. This is facilitated by the 'service access' mechanism. In traditional methods of service delivery, a service seeker needs to be present physically at the point of service that is generally delivered Over the Counter (OTC). Here, trust is established between the stakeholders through the visual inspection of a person and their documents. However, unfortunately, this means of establishing trust cannot be extended to electronic means. Therefore, one of the major challenges posed by electronic service delivery is how to establish that same trust. As this comes up at the point of service access, this is considered as a last mile challenge.

The fourth stage of the service delivery is issue and problem resolution. Disputes may arise and, hence, legally valid evidence of service access as well as of other various associated transactions is required to prove the validity of complaints. In addition, a history of service access and transactions may give insight into the behaviour of the overall e-government system. The above aspect along with business intelligence gathered through service analysis and reporting can result in the continuous improvement of e-government service

delivery. The following table summarises the challenges involved.

Table 1. Challenges Associated with the Four Stages of the Development of E-Government Services

Stage	Challenge
Service Aspect	How to innovate services leveraging new possibilities thrown open by technology advancements
	How to eliminate redundancies across agencies
	How to offer integrated services that cut across agencies.
Service Delivery	How to make services ubiquitous supporting multiple delivery channels.
	How to make service delivery inclusive to all classes of the population.

Service Access	How to securely establish trust between the service providers and citizens.
	How to ensure that the service delivered is in accordance with the entitlements of the citizen.
	How to record all the service access for future evidence in a legally valid manner.
Service Analysis & Reporting	How to generate crucial Business Intelligence (BI) from the analysis of the overall systemic behaviour over a period.

1.4 Stakeholder Perspectives

The following diagram summarizes the perspectives of government, business and citizens regarding e-government transformation:



Figure 4. Government, Business and Citizens Perspectives of E-Government Transformation

1.5 Striding Towards Alignment

Government agencies and departments have existed for a long period of time as silos so they now need to embrace a more collaborative view. It can be noted from different practices around the world that government departments embraced information and communication technologies as an enterprise level strategy rather than as a federal strategy. Hence, there are many differences in the technology maturity level across various departments. E-government transformation, though, requires the alignment at the federal as well as at the local levels in terms of technology, planning, coordinating monitoring and evaluating.

One of the key elements in moving towards alignment is the federal enterprise architecture. This would give a common technology ‘blue print’ for every department to follow while implementing ICT strategies. In addition, a set of interoperability standards would not only help the integration among the departments but would also enhance the sharing of information to make all services more efficient. All these strategies would be incapacitated if there was an absence of a shared infrastructure at the federal level. Really, the most important shared service at the federal level is identity and access management service.

1.6 Key Drivers and Enablers

A profound transformation to e-government brings in a basic holistic change in the way governments function and in the way citizens experience the services offered. A massive change of this scale needs to leverage both 'push and pull' factors. The push factor is through government enforcement with laws and regulations; whereas, the pull factor is when citizens and businesses demand such as change. The pull factor is more desirable as it helps to accelerate change in the desired direction. If that is the case, then we need to look at how a high momentum can be created with this the pull factor. When different segments of society start to perceive greater benefits, they become self-motivated to embrace the new environment. The following questions would typically arise from the citizen and business perspective:

Citizen

- ➔ Does it improve my quality of life?
- ➔ Is it more convenient?
- ➔ Can I get things done in less time?
- ➔ Does it mean I don't have to go to multiple departments or offices?
- ➔ Does it ensure that my full benefits reach me without any hindrances?
- ➔ Will the services be more predictable and responsive?
- ➔ Do I need to pay more for the services in the new system?

- ➔ Will the services be more predictable and responsive?
- ➔ Do I need to pay more for the services in the new system?

Business

- ➔ Can it reduce the cost of my operations?
- ➔ Can I get approvals and permits faster?
- ➔ Can I identify and authenticate my customers faster and in a reliable manner?
- ➔ Will it enable me to serve my customers in a more personalised manner?
- ➔ Can it substantially reduce fraud?
- ➔ Will the change be costly to implement?

If citizens and businesses are convinced that the benefits of the change are more valuable than the cost involved; they will come forward and demand the change. However, any fundamental change will be resisted by the inertia entrenched in the overall system. The first challenge to be overcome is this inertia. Thus, we need to adopt the push factor. With the necessary regulations and laws, the executive must bring sufficient thrust or initial momentum in order to overcome this inertia to provide a good start for the transformation. For a vehicle of change to reach the target goal faster in an efficient manner, the appropriate road needs to be taken. Similarly, e-government transformation needs certain enablers to be in place in order to progress smoothly. The following are some of the key enablers for the e-government transformation:

Critical shared infrastructure such as:

- ➔ National electronic authentication gateway
- ➔ Federated identity services
- ➔ Federal Public Key Infrastructure (PKI)

Centralized planning and coordination

Necessary technology and solution ecosystem

Availability of skilled resources

A blueprint for federal enterprise architecture

Federal interoperability standards and guidelines

Central monitoring and evaluation

1.7 Trust Establishment around the Globe

One of the major challenges facing electronic service delivery is how to establish trust between service providers and service seekers. This is, especially, difficult in cases where citizens can avail themselves of services unattended through self-service modes; trust needs to be established automatically and remotely to enable access to specific services. Here, technology comes to the aid in the form of smart card, PKI and biometrics. The e-identity uses these technologies in a well-rounded manner so as to leverage maximum potential. The e-Identity issuer also follows highly secure and efficient processes to establish identity assurance. This combination of systems, processes and technologies is designed to efficiently establish trust between citizens and government service delivery.

Over the last decade, Belgium, Finland, and Norway have led the digital revolution. These countries have transformed their government transactions and enabled many secure Government-to-citizen (G2C) internet-based service modelled transactions. Digital certificates issued to their citizens are key characteristics of these systems. The USA, under the Office of the CIO, has developed a comprehensive Identity and Credential Management Framework and is spearheading the implementation of a unified National Identity card.

The Middle East has taken a cautious approach as it seems to want to learn from other existing implementations in order to avoid the pitfalls of these early adopters and be able to successfully adopt already proven technologies in the field of identity management. The United States, the UK and most European countries have already implemented biometric identification systems to identify visitors and to transform border control mechanisms. South Korea, on the other hand, has issued a smart card to all its citizens and residents based on national identification systems that enables e-identity-based transactions. This smart card has validated identity and was verified by the Government. The UAE, Oman, Bahrain, Qatar, and many other countries in the Middle East have also launched multiple large scale biometric-based identity programs that provide secure and modern identity documents to their citizens and residents.

Overall, governments in the last decade have spent tremendous effort and some substantial financial expenditure to modernize their identity systems with the aim of developing compelling 'identity profiles' which strengthen security systems and protocols used across government agencies.

1.8 Conclusion

E-government transformation efforts are massive in scale and, at the same time, the modern day dictum is to provide a more personalised experience to citizens and residents. As traditional e-governments were transaction based, they treated citizens as an undifferentiated mass of customers. Each transaction was treated as a discrete service. The new age e-governments, though, need to move towards value creation through the long term engagement of citizens. Through the co-creation of value, e-government will undergo continuous improvement and provide a superior personalised experience to each citizen. In the transformed e-government scenario, establishing trust between the citizen and the government is of utmost importance.

One concern to be raised at this point is in a government's ability to create operational capacities that enable such a superior personalised experience for its citizens. Businesses have successfully overcome this challenge by outsourcing. This model has sufficiently proved that it is not necessary for business organizations as well as for public entities to own all the resource bases they require. What is important is how to build capacity to access the networks of resources by tapping into the global resource pool.

In the following chapters, the book will attempt to not only pin point the challenges involved in creating such a personalised-government experience, but it also recommends possible solution models and approaches.

2

FACTORS THAT ACCELERATE E-GOVERNANCE TRANSFORMATION



Figure 5: E-Government Conceptual Model

2. FACTORS THAT ACCELERATE E-GOVERNANCE TRANSFORMATION

It has been demonstrated that e-government transformation is seen in the light of 'citizen identity' and 'citizen relationship management' that serve as focal points. This chapter provides and describes a complete framework for e-government transformation acceleration. This describes the ability for e-governance to not only reach the citizen, but to stride alongside the citizen with the agility and mobility that is expected from regular face to face services, but now as e-services.

2.1 E-Government Conceptual Model

While attempting to build the solution models, it is important to have a conceptual foundation that conveys the overall aspects of the solution. In our water lifecycle model, the citizen service innovation strategy is absorbed by the agencies/service providers who translate these strategies into e-services for the citizens.

There is a greater need to aggregate and to transform the basic services offered by the agencies/service providers through integration and transformation. After the services have been transformed, the focus is on the delivery channels to take them to the doorstep of the citizens. Enablement at the users' end is also needed which allows

them to utilize the e-services and enjoy the benefits. In all these stages, the agencies/service providers get important feedback and inputs that generate Business Intelligence (BI), which in turn enables them to fine tune their policies and strategies.

2.2 E-Government Transformation

It thus may be seen that the aggregation of services and the transformation of the service delivery drives the e-government. The e-government initiatives then become dynamic in nature.

In this context, it would be good for us to understand the nature of dynamism in e-government. E-government models and e-governments have evolved. In the wake of the digital revolution and the ever changing technology landscape, it can be seen that e-government programs need to adopt and adapt the technologies quicker than ever before.

The ubiquitous presence of the mobile phone has now warranted that government services be available round the clock, enabling a true 24-hour government. Therefore, even if we scrutinize the first stage of an e-government program establishing an on-line presence, we find it to be in a state of flux. An online presence does not mean just on a website or a portal; it is now seen as 'presence' on every type of electronic and mobile device. This poses severe challenges to program implementation and marks the management of changing goal systems.

E-government has two major components - the 'e' part and the 'government' part. The 'e' part needs to now be looked at from the context of technology management; whereas, the 'government' part needs to be looked at from the context of connected government. Both parts contribute to enhancing the quality of life for the population. The 'e' part and the 'connected government' then need to converge to provide a seamless experience to the citizen. Thus, the technology needed for the e-government needs to be managed along with the governance needs. One major factor that facilitates this unification and the much sought after seamless experience is a uniform identity, which is accorded by the various national identity programs.

Central to any e-government program is the citizen. A national identification system typically provides a unique identity to the citizen. such identity is provided as a 'digital identity profile', it not only provides the citizen with the ability to transact in the digital medium, but it also serves as the citizen's common identification across all government departments. This is thus the unification factor that ensures the same primary key across all citizen and customer databases and enables the citizen to have a seamless experience across the government.

A formal framework for e-government transformation Management could then be proposed as explained next.

2.2.1 E-Government Transformation Management Framework

The dynamic nature of the framework objects is accentuated by the accelerators. The adoption of the accelerators then defines the roadmap and the speed at which the desired e-government transformation can be brought into play.

This E-government Transformation Management Framework seeks citizen welfare and happiness as focal point. The citizen is central to the government - after all, the government works for its citizens! The citizen-centric initiatives are backed by a clear value proposition and value realization to add incentive for investments.

This makes the Return on Investment (ROI) tangible alongside transparent performance monitoring. The value proposition is realized by the business impact as well as by the desired change necessitated and delivered due to the citizen focused initiatives.

Change Management thus plays a major role in the management of expectations and ensures a smooth transition to the desired state of a mature service delivery. This would further guarantee that the required resources are prepared and made available that would sustain the initiatives and that the satisfaction of the citizens would be continuously enhanced. interoperability of the government departments and the business process integration between the various agencies would determine the successful achievement of the outcome and would result in citizen satisfaction.

The technology adopted and the infrastructure, especially, the IT infrastructure and design architecture would need to consider the interoperability and service integration in order to deliver the citizen services effectively.

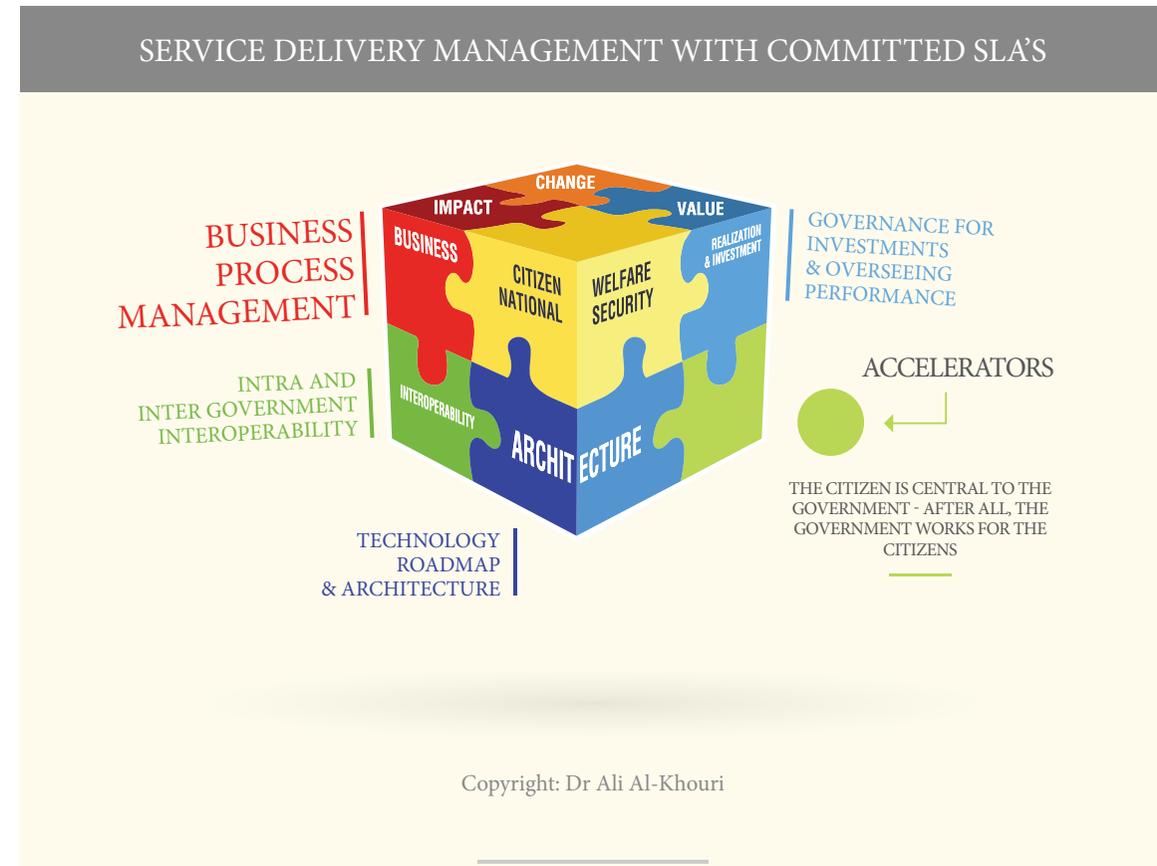


Figure 6: E-Government Transformation Management Framework

2.3 Push and Pull Factors

Let us now examine some of the influencing factors that contribute to the transformation of e-government within the context of the four stage service delivery model as well as the role of the demand and supply of services.

The first generation of e-government was technology-push oriented with more emphasis given to research and development (R&D). The implementation here assumed that scientific discovery preceded and 'pushed' technological adoption via applied research. The second generation was more need-pull based with more emphasis put on marketing. Thus, the market became the source of ideas for directing the R&D and leading it to play a more creative role in solving citizen problems.

In the next generation, a combination of push and pull with feedback loops dominated the market so that R&D and marketing were more in balance. More emphasis was placed on integration at the R&D/marketing interface. In the fourth generation, which proposed an integrated model, research and development became integral to teams of strong upstream service providers so that a close coupling with customers and partners was enabled.

In addition, horizontal collaborations (joint ventures, etc.) were promoted. The current fifth generation sees more integration between systems based on networked models that are supported by fully-integrated parallel development. A strong link with customers and a customer focus is at the forefront of this integrated service

development strategy. Horizontal links are well established with joint ventures, collaborative research groupings, and collaborative marketing arrangements, etc. In this mature scenario, regulation and technology are thus seen to be the major push factors while social demand and personalised experience constitute the major pull factors. A high uptake of e-government requires that more attention needs to be given to the 'pull mode'.

As we can see, the current e-government is based on a mix of technology push and social demand pull. Therefore, there is a general notion that any new social change should be supported by two factors: technology and demand. E-government is thought to be the field where this notion can be applied directly. In the public sector, a gap exists between social demand and institutionalisation. Legally, governments agencies have their own territories, which are quite well protected by high legal walls. These walls have prohibited government from adopting the networked solution approach and have also, to the detriment of the government and the public, prevented a smooth flow of information between organizations, agencies and departments.

If lagging institutionalization was inevitable, another alternative had to be found, which led to e-government's being the answer. E-government was a way to successfully make a detour around bureaucratic procedures. E-government became the way to remodel public management without significantly altering the organizational structure or the legal decision making process. Also, e-government made it possible to delegate the decision making authority to field officers.

While e-government stands to ease procedural wrangles, it has also attempted to transform the notion of security. Security issues in cyber-space are related to anonymity, which promotes 'stranger relationships' among people. e-government transformation thus seeks to work as the foundation of trust building in cyber-space where this 'stranger relationships' among people has been created. This transformation should ensure there is a system of trust in cyber-space as there is in the physical space.

2.4 Benefits of Delivery and Incentives

Thus, the push-pull factors resolve into benefits and incentives for the stake holders, which, in turn, would lead to the greater adoption of the e-government initiatives.

As an example, aiding the regulatory functions of the government, the deployment of information technology can offer benefits in the registration process of businesses, taxation, healthcare, education, and transportation, to mention only a few. These benefits could include higher revenues, increased coordination between government agencies, greater transparency in law enforcement and also a better compliance from constituents due to monitoring systems. Electronic service delivery provides benefits not only to citizens and businesses, but it also helps improve the image of the government, cut costs and advance the transparency of operations. For citizens, the main benefits of e-government are the more convenient, faster and efficient services and the faster gratification of service requests. Additionally, the costs for citizens are reduced;

the transparency is increased; governmental information is more easily accessible and the quality of life is enhanced. Businesses gain similar benefits from e-government, namely, reduced costs and an increased transparency as well as increased business transactions. Furthermore, businesses gain from the higher speed of business processes and higher transaction throughputs due to the new ease of interaction with government agencies, more simplified business transactions with government and a more supportive investment climate.

Another example is that electronic justice systems aim to integrate the various judicial and other organizations of a country or a region to provide more efficient justice. In such an electronic system, institutions such as police, prisons and courts are networked so that the necessary paperwork can be reduced, the processing time of cases is quicker and, more generally, mistakes in the judicial process can be minimized or eliminated and corruption curbed.

2.5 Out-of-the Box e-Service Innovation

Innovation in the public sector is driven by various factors both inside and outside the organization. The demands on the innovation requirements range from changes in government policy, stakeholder demands, and new developments in technology for agencies and individuals seeking opportunities to improvise and optimize the way they work. There will always be internal and external pressures on the public sector to innovate. The level of innovation will most likely increase and be sustained; if it is actively encouraged, recognized

and rewarded by organizations. Pro-active executive leadership, a supportive culture, a focused corporate strategy and investment in staff training and development are essential preconditions for innovation.

The idea of innovation in the public sector has evolved alongside a more nuanced understanding of innovation, as something that encompasses non-technological processes and the service industry, in addition to its more traditional meaning of technological innovations. There are five types of innovation:

- ➔ **Innovation** that involves changes in the characteristics and the design of service products as well as in the production processes - including development, use and adaptation of relevant technologies.
- ➔ **Delivery innovations** involve new or altered ways to solve tasks, deliver services or otherwise interact with clients for the purpose of supplying specific services.
- ➔ **Administrative and organizational innovations** involve new or altered ways of organizing activities within the supplier organization.
- ➔ **Conceptual innovation** is in the sense of introducing new missions, new worldviews, object strategies and rationale.
- ➔ **System interaction innovations** involve new or improved ways of interacting with other organizations and knowledge bases.

Innovation management in the public sector should be principally aimed at addressing societal challenges, since these are the major challenges that require high public effort. Accordingly, innovative thinking and operating may require strong user-centred approaches and involve a deep knowledge base and expertise. Citizen empowerment is a key aspect for ensuring ex-ante value-driven and universally acceptable solutions. For this reason, it would be beneficial to collaborate with civil society representatives and NGOs. Large scale experimentation and testing methods can also be implemented to enable citizen empowerment through the use of information and communication technologies.

The challenge of scale up from pilot projects or prototypes has to be handled with care as a wrongly calibrated or poorly calibrated sample could result in production scale failures. For the public sector as a whole, the adoption and diffusion of innovations matters even more than innovation itself. Successful small scale experiences have sometimes been rapidly written off because of a lack of connectivity and relevance to the larger population, which resulted in no acknowledgement or appreciation of added-value. Furthermore, it has been noted that innovations are often slow to spread owing to their having poor incentives to their being adopted as well as other cognitive barriers, which impede their diffusion. Here again, innovation management processes face problems of both horizontal and vertical silos where even strong networking can be an insufficient solution.

There are different barriers for innovation such as social, financial and technical phenomena, which hinder innovation activities in institutions. These can be:

➔ **Professional resistance and heritage:** The public sector is often characterised by professional groupings with their own communities of practice, established roles, and their associated policy agendas. As such, there may be a reticence to embrace change and innovation, especially, when it is external innovation (from another organization or the private sector). The systemic impact of innovation and change is often viewed as an unwelcome hindrance to the overall functioning of the organization. A lack of dialogue between the different parts of the public system, horizontally or vertically, and between different professional groups may also hold back innovation and its dissemination.

➔ **Absence or inadequacy of resources:** This feature is generally considered as the main barrier to innovation. Resources include, not only a lack of financial support, either in a general context or specifically for the support of innovation, but they can also include shortages in relevant skills, in human resources or for enlisting other support services that may be required for the implementation of the innovations.

➔ **Public resistance to change:** It is assumed that the public is, in general, resistant to reorganization and changes in the way public services are delivered. Thus, the public, or elements

of it, may also be risk averse. This resistance is expected to be particularly strong when the public is not informed enough about the benefits of the changes and their direct impact on them. However, some types of change might be more welcomed than others, by the users of the services or other public stakeholders.

➔ **Pace and scale of change:** Many public administrations and services have been subject to a large number of radical changes, often called reforms. These often lead to an unstable environment with no medium or long-term visibility so employees have little opportunity to reflect upon and assess the impact of the innovations introduced. Thus, many people become 'innovation fatigued'.

➔ **Size and complexity:** The public sector is comprised of complex, large-scale organizational entities that may develop internal barriers to innovation. These barriers can consist of localized skills, shortages and gaps, a lack of clear agreement as well as communication difficulties. Within such settings, small successful innovations may hardly be diffused or scaled-up.

➔ **Risk aversion and accountability:** There is an understandable inherent reticence (especially concerning healthcare, and transport, etc.) to undertake or implement changes, which may result in the increased probability of risk for users and civil servants. In addition, public organizations scrutinised by politicians, the media and employees are not normally rewarded for taking risks. Consequently, public service managers and politicians are wary of enacting changes that may result in negative outcomes. There may also

be a tendency towards a blame culture, with its associated high levels of accountability, which can be exacerbated by the difficulties in obtaining a clear picture of all the potential effect and impact of these actions.

➔ **Technical barriers:** There may be a lack of technological solutions to the problem at hand. The application of new uses for existing equipment, for example, could push the technology to the limits of its capabilities and act as a driver for further technical innovation. On the other hand, it is sometimes argued that too much emphasis is put on the technical aspects of the implementation process whereas these should not be considered as innovation by themselves as they can also bring new obstacles.

➔ **Absence of capacity for organizational learning:** There may be a lack of structures or mechanisms for the enhancement of organizational learning and the diffusion of good practices. The reasons for this are broad and manifold: a frequent reorganization and staff turnover, a tradition of secrecy, a lack of evaluation of previous policies and a rigid top-down command chain.

While an innovative idea can result from serendipitous events, embedding a systematic approach as an explicit and integral component of an organization's corporate strategy would drive the development and promulgation of appropriate policies and procedures, the allocation of necessary resources, the assessment of results and the dissemination of knowledge.

An innovation strategy that is clearly articulated, readily understandable and relevant to all levels within an organization is likely to have more impact in raising innovation performance than not having such a strategy. The appropriate innovation strategy depends on the organization. The possible strategy may, on the one hand, tend towards approaches that focus on generating innovation inside the organization or, on the other hand, tend towards approaches that focus outside the organization. For some organizations, innovation policies are also supported by policies dealing with intellectual property.

Thus, the management of innovation needs to be seen in the context of the government's and the community's desire for more citizen-focused service delivery. This can provide significant opportunities for innovation. Innovation thus needs to consider the social inclusion agenda in order to provide a comprehensive, united delivery of service.

Of course, these challenges for innovation concerning e-government transformation are not trivial, but they can be overcome through a coordinated collaboration effort and by partnerships across agencies. Innovation initiatives can be viewed from new and enhanced delivery mechanisms, through redefining the role and responsibilities of redesigned back office processes using enhanced IT platforms and simplifying the customer interaction process. All of these ease a citizen's communication and transaction ability as a customer of the government.

2.6 Anywhere Anytime Access

An e-government accessible anywhere anytime has to fulfil this commitment of constant availability, as well as context-awareness and environment integration. The following are some of the characteristics of this kind of ubiquitous government (Dutta and Bilbao-Osorio 2012):

- Accessibility and availability at any necessary time and place.
- Acquisition, analysis and usage of context to provide more efficient, personalized services.
- Seamless interaction for the user.

‘Digital divide’ is defined as ‘the gap between different individuals, households, businesses and geographical areas at different social-economic levels regarding their opportunities to access IT and their use of the Internet’. It is widely suggested that ‘digital divide’ is a key risk factor in e-government projects, among those of project size, newness of technology and project structure. In recent years, digital divide has become an increasingly popular subject in policy discourses, academic research and civil society debates around the world.

Countries around the world have invested heavily in the infrastructure of information technology based on the assumption that by achieving a solid infrastructure level, the benefits of information technology would flow automatically to citizens, businesses and governments. This assumption essentially means that overcoming the connectivity

gap would bridge the digital divide. However, while connectivity is a prerequisite in reaping the benefits of ICT, it is not a sufficient condition by itself.

For those who use computers, they are finding that browsing is becoming more ‘seamless’ or ‘transparent’. In a ubiquitous anywhere anytime government, technology serves ‘as a means to an end’ and, therefore, should ‘take a back seat to allow users to fully concentrate on the task at hand’. Although technology is becoming more unobtrusive and seamless so that it is almost “hidden” from users; it is after all technology-dominant. The provision of public services, on the other hand, is citizen-centric. This means that computing only serves those people who use computers. However, governments cannot choose their customers - they are obliged to serve all citizens computer literate or not. As a result, governments must meet the digital divide challenge.

In addition, the notion of ‘existing everywhere’ applies to service provision or availability ‘at hand’, but it does not address service accessibility, which is of equal importance. In situations where public services indeed actually ‘exist everywhere’ through online channels; the digital divide could well deter some citizens from gaining access to these services. The noticeable presence then of the digital divide puts constraints on ubiquity in terms of government service provision, which, in turn, makes ubiquitous government less meaningful. Without citizen accessibility, service availability by itself cannot realize the full benefits of a ubiquitous government.

For primarily older citizens who lack the motivation to adapt to the use of online services, actual service utilization can be assessed and fostered by using adequate channel management strategies, which can be defined as strategies used to switch users from a certain channel of service distribution to an alternative channel. Examples of this include providing sufficient incentives and eliminating (discontinuing) conventional offline channels. In comparison, building a digital inclusive society that takes into consideration the digital divide among citizens is far more challenging.

A 'digital inclusive society' creates a society where citizens can explore the potential and benefits of new technologies, access and share information and services freely and effectively, as well as participate in the community through the use of ICTs. These highlight the motivation for exploring available ICTs and point out the importance of accessibility and participation. In this connection, government services should be delivered ubiquitously in an accessible manner.

Built upon their analysis, we can reflect upon the time when all government services were delivered through conventional offline channels. While ICT is enabling governments to deliver services and approach their citizens in a wide variety of channels, the conventional channels certainly remain appropriate in many service scenarios and some are actually still more effective.

The advancements of Information and Communication Technologies (ICTs) have not only given rise to the era of e-government, but they have also revolutionized the way

governments deliver services to their citizens. These advancements allow governments to make their services available and accessible to citizens in a ubiquitous manner. According to our analysis, the notion of ubiquitous must be expanded to refer to far 'beyond the constraints of time, place and digital divide'. In such a case, accessibility is the key factor so equally important to the others.

In a ubiquitous government, providing government services through the conventional, offline means becomes inseparable. For improved service, availability and accessibility are critical to attaining the ultimate ubiquity, (thus) an appropriate mix of online services and offline services is pragmatic and essential. This suggests that a ubiquitous government be a superset of e-government. The 'right' mix of online and offline services may be specific to service scenarios and can evolve over time. Hence, policymakers and researchers should put their effort into designing an optimal mix with respect to the target service scenario rather than focusing on online channels exclusively.

Designs of e-government solutions should consider more how to improve the integration of online processing and offline channels, thereby achieving greater synergy and minimizing wasteful resource allocations, which result from the maintenance of dual channels. In addition, delivery channels should be vertically separated from delivery interface and backend processing. While the backend processing can benefit from the digitalization in e-government, the delivery interface should match the citizens' needs and preferences. Equipped with the facilitating backend processing and an effective interface for service delivery, governments can alleviate the

magnitude and the prevalence of digital divide, thus realizing the grand vision of a digital, inclusive society.

It is argued that successful e-government only happens based on how it affects different parties and the various benefits it offers to its multiple stakeholders. The provision of government services through multiple media such as the Internet, mobile phones, digital TV, etc., allows for a greater penetration and so greater benefits for citizens, in the areas of mobility and the reduction of the digital divide.

A personalization of services based on user data and context provides citizens with even more convenience and efficiency. Embedding technology into everyday life allows for new user experiences and promises benefits for the less technically capable users as well. For governments, ubiquitous services can improve their image even more.

Geographic location would no longer be relevant due to the ubiquitous technologies so the citizens would be free to cross borders, and access services anywhere, at any time and participate in decision-making. This scenario also takes in the proliferation of biometric identification, smart cards, sensors and mobile technologies.

Of course, mobile devices are now one of the most common new platforms for offering government services. As a step towards these ubiquitous services, mobile devices can provide them to a wider audience at any given time. The multitude and different parameters of mobile devices do, however, make it harder for governments to provide the same services on so many different platforms.

The penetration of mobile phones is said to be the highest among any ICTs with regard to the world population and it is increasing. Although, mostly used for just voice communication, mobile phones today allow for many other applications like text and multimedia messaging and Internet browsing.

2.7 Personalized Experience

The key phenomenon in e-government is the gradual personalization of social services. Thus, services for elderly, special education or pension reform will all have search features that can tailor the services to the needs of these specific individuals, with the added possibility of choice. Here, the responsibility for a person's own social status is shifted onto the citizen and his/her ability to choose among various possibilities. For special education purposes, specially designed instructions and services provided by the school district or other local education agency would aspire to meet the unique needs of students identified as challenged. Special education may include instruction in a general education or special education classroom.

In transition countries, the shift in philosophy, towards citizen-centric, has become the centre of all the innovative effort that has focused on the 'humanization' of the environment, a gradual de-institutionalisation of social care and the improvement of the relations between the staff / facility and the client. This innovative approach in the transition context reflects on a range of new features that span from the creation of alternative services, physical improvements in the facilities, the introduction of new

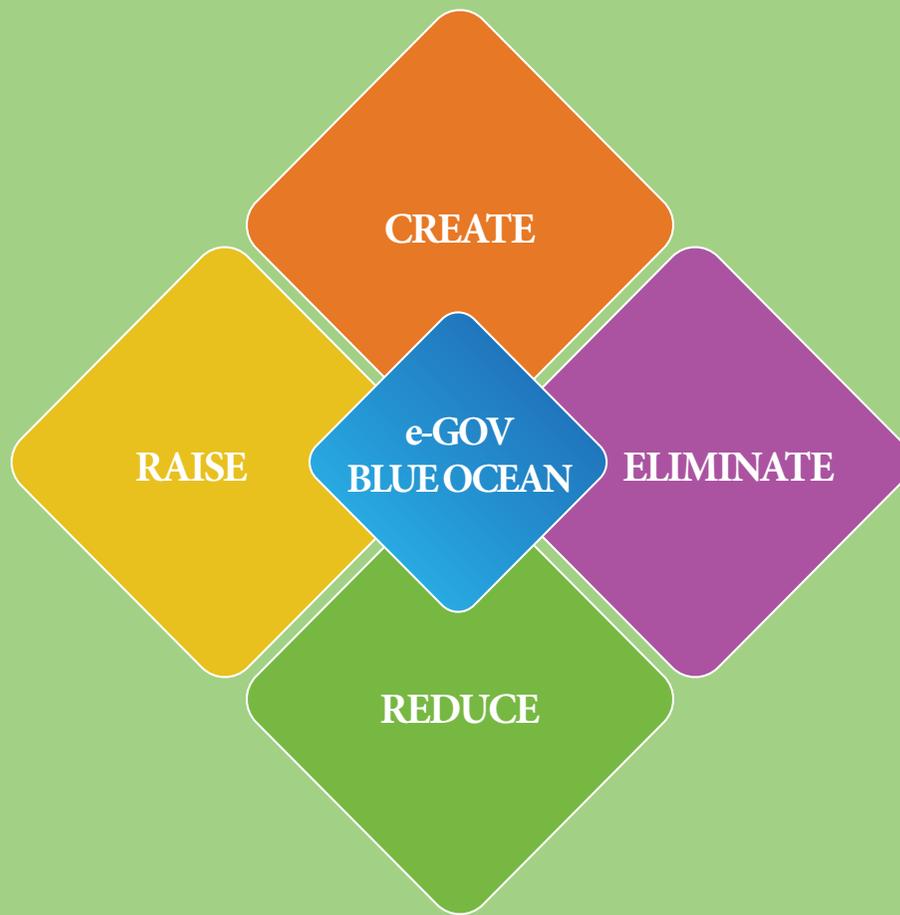


Figure 7: EERC Grid of E-Government

(personalized) services according to the client's needs and the related free-time activities for senior citizens, as well as to the introduction of quality standards and performance management that would all secure minimum standards in the services provided.

2.8 Blue Ocean Strategy for Value Innovation

The most appropriate unit of analysis to explain the Blue Ocean Strategy is by the strategic move. The creation of a Blue Ocean Strategy builds brands. So powerful is this strategy that a Blue Ocean move can create brand equity that lasts decades (Chan and Mauborgne, 2005).

Several driving forces are behind the rising imperative to create Blue Oceans in the e-government domain. All the accelerated technological advances have substantially improved industrial productivity thus allowing suppliers to produce an unprecedented array of products and services. The result is that, in an increasing numbers of industries, supply exceeds demand.

The creators of Blue Ocean didn't use the competition as their benchmark. Instead, they followed a different strategic logic called 'value innovation', which is actually the cornerstone of the Blue Ocean strategy. Thus, the public sector service innovation falls under Blue Ocean strategy. In the context of governments, it is not a question of competition; Blue Ocean is concerned with value creation, which can then open up new and uncontested market spaces and opportunities

that propel citizen happiness and national growth.

The most fundamental tool of the Blue Ocean strategy is 'the strategy canvas', which has a four-step process to help practitioners come up with their own Blue Ocean strategy. To apply this strategy to enable government to promote e-government transformation, the following steps based on the strategy tools and frameworks are suggested:

The first step is the visual awakening, where a government evaluates itself with leaders. The second process is known as visual exploration, where government strategists talk to citizens and civic society groups to find 'pain' points which reveal where the government strategy needs to change. The third process is the visual strategy fair which basically asks the following questions: Which of the factors that the citizens and businesses take for granted should be ELIMINATED? Which factors should be REDUCED below the industry's standard? Which factors should be RAISED well above the industry's standard? Which factors should be CREATED that the industry has never offered? These questions can be answered by using an Eliminate, Reduce, Raise and Create (EERC) grid.

Eliminate (E): Government can simplify and automate business processes thus eliminating paperwork. Simplified processes mean less paper cost for the government, less manpower to receive and process the forms, less rental to house the people who file the paper.

Reduce (R): The reduction of bureaucracies and laws that hamper the citizens and businesses can be done in at least two ways - by rewarding government employees who can identify obsolete

laws, thus reducing potential corruption due to the ignorance and/or confusion of the existing laws in the various government departments and bureaus. The second type or reduction is for the leadership of the legislative department to encourage proponents of new laws to identify as many obsolete laws that can be superseded with the introduction of the new proposed ones. The manner of helping entrepreneurs to identify and thus abolish obsolete laws will trigger a tipping point for other obsolete laws to be identified and abolished as well.

Raise (R): Encourage incentives for the creation of public private partnership in e-service innovation and for those who invest in training and human resource development.

Create (C): Digital inclusion must be brought about by enabling all citizens to access and participate in a transformed e-government. The government can then focus on only investing in those things that will make the new strategy canvas a reality, as well as in building a customer-centric organization where civil servants will not just be listening, but will be relevant to the needs of the citizens and businesses.

2.9 E-Government Transformation Acceleration Framework

Based on these influencing factors, the e-government Acceleration

ACCELERATORS

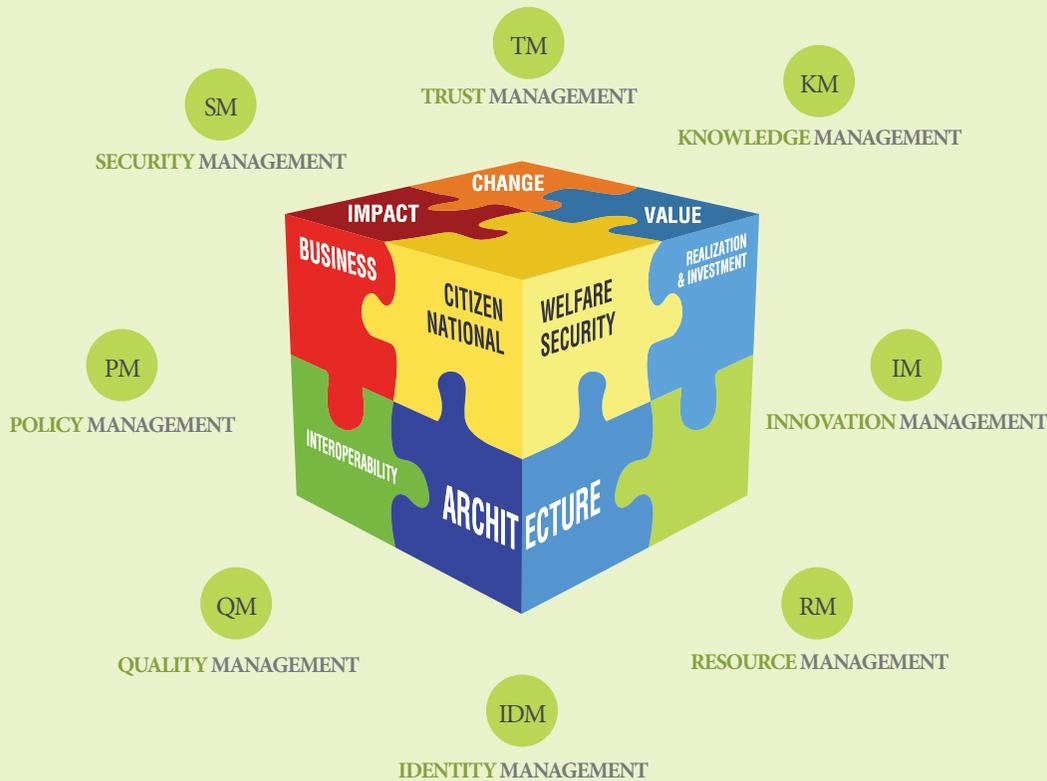


Figure 8: E-Government Transformation Acceleration Framework

Framework would be developed. The accelerators are purported to be basic in nature and strongly contributing to the pace of transformation.

The e-government Transformation is not organic, but needs to be managed in order to deliver the strategic objectives and goals of the government with the citizen as the focal point.

While the transformation itself needs a carefully coordinated effort among the different agencies, it calls for a national level management. From the e-government Transformation Management framework depicted earlier, it can be noted that many factors contribute to this transformation. More importantly, the following factors tend to influence the pace of the transformation itself. These are what one could call the e-government Transformation Accelerators. To sum up the above discussion, these accelerators could be depicted as in Figure 8.

These form the basic accelerators that contribute to quickening the pace of the e-government transformation. Therefore, managing these factors determines the pace of the transformation. Central to these factors is the identity management. Many national identification programs around the world have been based on the concept of providing the necessary identity documents for both citizens and residents thus according them their rights of existence in the country. Such identity management systems strive to provide irrefutable proof of identity for its citizens and provides the core of the integration for the government services. The citizen thus has a unified identity across government departments and agencies that enables them to have seamless transactions that facilitate government-to-citizen (G2C) and government-to-government (G2G) transactions.

This would in turn contribute largely to the management of security and trust. Security lies not only in protecting the citizen's data and privacy, but also in ensuring the accessibility and integrity of the information. As more and more services get e-enabled and government services become ubiquitously available, it is imperative to establish a high level of trust in remote transactions. Identity credentials thus play a major role in trust enablement and managing the required trust in the transactions contributes to a successful e-government.

The corner stone of e-government transformation is innovation and knowledge. Managing innovation and knowledge in the national context assumes huge proportions and a government's active support in these areas vastly contributes to the pace of the transformation. Skilled resources as a national human capital

pool then drives the management of knowledge and enables governments to innovate.

The e-government transformation is further impacted by national policies. Cyber-protection, the regulation of financial transactions in the virtual channels of transaction, the legal system that strengthens the digital transactions and the active participation of law enforcement agencies go a long way in building consumer and service provider confidence that leads to remote transactions.

Quality Management seeks to raise the standardization of implementation and ensures the interoperability of different service provisioning systems.

The prioritization, application and detailing of the accelerators depends on the socio-economic environment in a country. The adoption of the accelerators then dictates the pace of transformation. The following section will examine briefly the key success factors that enable this adoption.

2.10 Key Success Factors

Information technology (IT) has the potential to transform government structures and to improve the quality of government services. This technology provides two main opportunities for government:

- (1) Increased operational efficiency by reducing costs and increasing productivity.
- (2) Better quality of services provided by government agencies.

Realizing the benefits of these technologies requires the organizations to understand and overcome the challenges to their efforts. Technological complexity and incompatibility are not the only, nor the most difficult, challenges to overcome. Managerial, political, and legal factors have also been identified as important elements to take into consideration in the design and development of IT initiatives. Politics, privacy concerns, turf, and other institutional arrangements can also affect the results of an IT project. The following list includes the most prominent success factors for any e-government transformation:

- **Internal political desire:** This has been defined as the drive from key government officials including relevant ministers for reform and for achievement of e-government goals.
- **Overall vision and strategy:** This stands for the overall vision and master plan for good governance and for e-government, by identifying the target and viewing IT as the means not the end, and integrating IT with broader reform objectives.
- **Dominance of politics/self-interest:** The change agents who will take the project forward may have a self-interest and/or politically dominate the situation favourable to the project initiative.

- **Strong change management:** This includes, but is not limited to leadership with a project champion; the use of incentives to create commitment to and the ownership of an e-government project, and stakeholder involvement to build support and minimize resistance.

- **Effective project management:** This includes defining clear responsibilities, having good planning and a consideration of risk, good monitoring and a control system in place, good organization of resources, and well-managed partnerships between public agencies, and public-private joint initiatives.

- **Competencies among the officials involved with the project:** This involves the issues of the capacity and knowledge level of the government officials regarding e-government concepts and practices.

- **Adequate technological infrastructure:** This includes a computerized system, telecom policies, and ICT policies etc.

For governments to deliver their promise of service and availability to their citizens, necessitates a comprehensive strategy by which to implement the e-government initiatives. Many an initiative has failed due to the lack of such a comprehensive e-government transformation strategy. The following chapter seeks to address this challenge and proposes an adoption of an integrated strategy.

3

AN INTEGRATED TRANSFORMATION STRATEGY

3. AN INTEGRATED TRANSFORMATION STRATEGY

A key step forward in the evolution of governance would be the strategic integration of e-governance transformation. This chapter defines the strategic framework to achieve the objective and enumerates various global experiences in strategically integrating the e-governance transformation.

3.1 Integrated Strategy for an Integrated Vision

Many governments have achieved substantial progress in their e-government initiatives during the last decade. E-government has thus become a world phenomenon. Each government has developed its own strategy to meet the challenges of their move towards e-government development. Nonetheless, the realization of e-government in its full potential is still far from complete. Since it is still 'a work in progress', e-government is constantly developing. Therefore, e-government strategies are updated fairly frequently. This means that what was valid a few years ago in terms of service delivery, efficiency, etc., may not be satisfactory today. This is mainly due to the rapid innovation of newer technologies and ideas.

Throughout the world, all e-government strategies include a vision right at the beginning. A vision and political will are indispensable

for launching any e-government project. Vision is necessary, as it will always be the motto of the e-government department overseeing the overall program, which is normally responsible for planning and spearheading the implementation. This vision will always be referred to during the implementation later on. The vision is important as well because it reflects the policy of the government. From this vision, the committee is held accountable for outlining the mission statement, which is normally more expressive than the vision as it will contain further details.

Each government has certain extremely important objectives that it seeks to achieve from the development of its e-government program. These objectives justify the huge outlay of resources that must often be dedicated to e-government initiatives. The people responsible for the inception and development of the e-government must thus work hard to convince decision makers about the level of change required to make their e-government strategies successful - specifically in complex and politically sensitive areas.

Without support from its own leadership, the e-government is doomed to failure. Therefore, the justification of the strategic objectives is critical for the success of e-government initiatives. Thus, greater care must be taken, to devise the objectives in a coherent manner. The strategic objectives thus should provide a complete package regarding what the government wants to achieve. These objectives must never be totally unrelated or completely disconnected. For any viable implementation to take place, the objectives and their justification must provide some a definite universal focus that reflects a general direction behind the initiative.

Some of the important strategic objectives for e-government transformation are:

- Develop strategies to know the customer much better.
- Provide consistent service and information across all channels.
- Develop a multi-channel strategy that facilitates movement to new channels.
- Understand citizen interaction preferences and anticipate changes.
- Enable and empower employees to serve better.

According to the International Data Corporation (IDC), smart government is about “the implementation of a set of business processes and underlying information technology capabilities that enable information to flow seamlessly across government agencies and programs to become intuitive in providing high quality citizen services across all government programs and activity domains.” To transcend into smart government, government organizations need to know their citizens’ communication preferences in order to better connect with their customers.

More and more citizens prefer to interact with government over electronic channels. The ever increasing adoption of rapid smart mobile devices will have a deep impact on these preferences. Hence, governments should look at their customer preferences for interaction and then redirect resources from the less preferred /more costly channels to the preferred, less costly, and widely accessible channels. The following are the three dimensions of an integrated

e-government transformation strategy - also referred to as the Environment, Readiness and Usage (ERU) Framework.

➔ Environment

This is to do with the existing country-wide social, cultural, and political conditions for establishing an e-government system. As part of this dimension, a comprehensive set of laws must be passed that allow the government to leverage the full potential of automation and online service provision while ensuring consumer protection, privacy, and security. Specifically, legislation is needed that can create a favourable environment for promoting trusted government, business, and individual activities over the Internet.

Moreover, these laws are required to also remove barriers to e-government and e-commerce that were raised by outdated laws and regulations. Additional goals for this dimension include enhancing information and communication technology adoption rates by individuals, businesses, and government entities; using technology to support collaboration, promote knowledge sharing within the government, and conduct awareness campaigns to increase adoption; as well as providing the e-government strategy owner with the right mandate to effectuate change.

➔ Readiness

In this dimension, the capabilities of a government to deliver best-in-class services to users and to leverage technology to tap

internal efficiency gains are assessed and any weaknesses are ameliorated. Both, the flexibility of the organizational culture and the sophistication of the information and communication technology infrastructure are addressed.

From a transformation management perspective, technological readiness involves building key enablers to deploy services, which include components that are provided centrally as well as decentralised components, i.e., components provided by individual government entities, but shared across multiple government entities. Organizational readiness focuses on the coordination and the deployment of skills across the government.

The interplay of technological and organizational readiness is necessary to ensure a broad-based e-government program that eliminates 'silos', which exist in many government bodies today. The silos are replaced with collaboration and knowledge sharing, as well as with the development of appropriate capabilities, such as high-level, cross-functional IT skills that are needed to manage a full-fledged e-government system.

The targeted capabilities that foster the modernization of e-government include supporting the standardization of processes to improve quality and increase predictability; attracting, retaining, and developing talented individuals who can deliver IT excellence; backing the design and delivery of standards based, shared, resilient, and secure architecture, infrastructure, and applications;

and establishing governance, interaction models, and processes to support the development of the IT strategy.

➔ Usage

This dimension emphasizes citizen-centric services and provides these services via multiple access channels; whereas, the environment and readiness dimensions address the requirements that are most effective across government entities, the usage dimension exclusively deals with service-specific requirements for each government entity. With this service orientation, the usage dimension is at the heart of the (ERU) framework, which determines and drives the requirements and needs for both the environment and readiness dimensions.

End-user-focused interaction models and service delivery channels are defined and adopted for implementation. Separate e-enabled applications must be developed to interact with the discretely different constituencies for which governments must provide services, e.g., citizens, businesses, other governments, and government employees. In this way, online services are always available, with service delivery across all access channels automated in the back office. To that end, an access model that offers multiple channels with a consistent customer experience in quality, design, and usability is necessary.

Areas covered by this dimension include delivering clear service

portfolios, often bundled from different organizations, according to users' needs, as well as providing a consistently high quality customer experience through automation, user-focused processes, and advanced staff capabilities.

3.2 Integrated Approach – Global Experiences

The misunderstanding that e-government mainly revolves around technological issues still prevails. In reality, the development of the information society is mainly a story of political will, organizational reforms, legal framework adoption, and reengineering work processes, etc. It has also been observed in many examples that the development of best practices is very closely dependent on the driving power of an organization's top management - both political and administrative.

Let us examine a few governments to actually see what has been achieved in this area.

3.2.1 Germany

Germany's IT Investment Program is aimed at four main areas - IT security, improving federal IT organization, Green IT and sustainability/innovation. The program includes over 300 individual inter-ministerial and ministry-specific measures such as setting up a green IT competence centre, providing the federal administration

with encrypted mobile phones and PDAs, providing a subsidy for infrastructure components (card readers, security software, electronic signature) to use electronic cards, promoting open source software projects for the entire federal administration, and promoting e-participation, etc.

An inter-governmental agreement included in German legislation covers the planning, development, and operation of the IT systems required for effective performance. This agreement supports the establishment of an IT planning council that is charged with developing the technical requirements for the core network infrastructure to be used. It will also have the responsibility for steering cross-disciplined e-government projects, along with making decisions about IT interoperability and security standards.

Another important aspect is the design of the future German identity card, which is based on smartcard and PKI technologies. The new card aims to ease citizens' transactions with government and businesses, increase security, as well as enhance public confidence in electronic services.

3.2.2 Belgium

The e-government program development in Belgium began to take off at the end of the 1990s. The program grew in response to the rapid development of the Internet and the increased use of ICT, which has also been seen in other advanced e-government OECD countries. E-government development has been dispersed throughout the government, with significant differences in approach, scope and

speed due to the considerable variations in administration size and the resources allocated to e-government.

With respect to full online availability of services for businesses and citizens, Belgium has considerably improved its position in international benchmarks. Formally, the Inter-governmental Co-operation Agreements define the framework for the collaboration and co-ordination among the Belgian governmental bodies, and support a common prioritised goal across and within governments: delivering integrated services.

3.2.3 Estonia

The Estonian e-government initiative seems structured around the adoption of the national identification system which provides a 'digital identity' profile with digital credentials for the citizens.

This identity card project focused on the digital signature is legally equivalent to the hand-written signature. At the same time, the technologies and standards for creating the digital signature have been made uniform throughout the country. The signature identifies a person directly, which eases the verification of signatures without additional contact. To achieve this goal, the Identity Documents Act, as well as the Digital Signatures Act was adjusted. This resulted in the following:

- ➔ The certificate inserted in the identity card includes the personal identification code, which enables the authorities to identify the individual at once.

- ➔ A certificate, which enables one to sign documents according to the Digital Signatures Act, is inserted in the identity card chip.

- ➔ Certificates inserted in the identity card lack the field of 'use restrictions' and can, therefore, be applied in the public as well as the private sector, as well as in the context of mutual relations between individuals.

The primary purpose of the information on the identity card chip is to allow the unambiguous digital identification of the individual and the creation of the digital signature. The certificate includes only the minimum information about the individual - name and their personal identification code. A firm decision was made from the start not to add additional information to the identity card, and, especially, not to mention information that requires updating.

The identity card is used in a general context, wherever or whenever a person needs to be authenticated or when documents have to be signed. This means that the identity card has not been created just for a certain service or application.

3.2.4 Singapore

The government has implemented an Internet based one-stop application system for business licenses. On a single Web page, individuals can fill out a single form to immediately apply for any number of licenses, even across multiple agencies; they can

then receive status updates about their applications via text or e-mail. This streamlined system is not only popular with business people, who are happy to sidestep Singapore's well-known and oft-criticized bureaucracy, but it also has had some tangible returns for the government: with as much as a 90% reduction in processing time, a 50% reduction in data entry, and - because redundancy has been minimized, a 10% reduction in licenses issued.

3.2.5 Bahrain

Bahrain's e-government system, which had its debut a few years ago, is an excellent model for how a government can transform itself into a service delivery organization. Citizens there were continually involved in the Transformation process - from formulating the strategy through to providing feedback, as the program was being set up. Ministers and senior government officials have established an open-door policy for interacting with their citizens, and the e-government program is ubiquitous on social networking sites such as Facebook and YouTube. In addition, the national portal and ministry websites provide features such as open forums, blogs, live chats, online polls, e-newsletters, and other interactive services that involve citizens in government decision making.

3.2.6 Canada

A program called Service Canada provides a good illustration of a full panoply of channels and offerings. This service has achieved a consistently high satisfaction rate (83%) among its customers

across all regions and program areas. In all e-government implementations, the decisive factors behind customer satisfaction are first and foremost the protection of personal information, followed by how well the system responds to the needs of individuals; as well as knowledgeable, competent, and consistent information; and the time that it takes for people to receive the service they are seeking.

As information quality, accessibility, and timeliness are not limited to e-channels, it's not surprising that there are still many e-government systems accessed via phone (by far the most dominant platform used), by fax, and in person. All of these channels, including the computerized ones, should be considered complementary, with each channel tailored to the user's preferences. Service Canada has implemented this almost perfectly. Despite the many remote ways to access the e-government system, Service Canada also offers all Canadians the opportunity for in-person contact within a maximum of 31 miles.

3.2.7 The United Arab Emirates (UAE)

The UAE is considered among the highest investing governments in its adopting and implementing progressive ICT in its government and private sectors. The UAE has recently announced a revised e-government Transformation Strategic Framework. This framework comprises numerous strategic initiatives at a federal level to transform all government services in order to make them available electronically through the various channels.

The e-government development approach in the UAE took into account three primary dimensions of e-services, e-readiness, and ICT environment. The e-service dimension is concerned with the acceleration of the pace of the e-transformation within government organizations and the provision of high quality electronic services through innovative delivery channels, e.g., Internet, fixed and mobile phones and kiosks, besides the traditional service centres. e-readiness focuses on strengthening the capacities of federal agencies in terms of ICT, organizational structures, HR capabilities and competencies, and their readiness for e-transformation. The ICT environment dimension covers organizational factors such as policies and legislations needed to support the implementation of e-government initiatives.

The e-government initiative in the UAE is largely focused on providing government services on the web and is aided by the national identification system and on the delivery of digital identity credentials to all the citizens and residents of the country. The smart government initiatives in the UAE are now poised to propel the country to bringing the government to the mobiles of the population, thereby, providing anytime, anywhere access.

3.2.8 The USA

A creative multi-channel system was launched recently in California.

The state's Web portal serves as a site for interactive communication with residents, and handles such activities as reserving a campsite

in state parks, applying for licenses, filling out employment applications, registering complaints against a business, and requesting a government loan. At the same time, iPhone apps are available for finding government offices, traffic and smog reports, and public transportation information. In terms of popularity, New York's 311 contact centre, a website and phone number for quick access to New York City government services and information, ranks extremely high. Overall, the system covers more than 2,000 services, the website handles hundreds of thousands of unique visitors a month, and the phone centre receives 40,000 calls every day, and responds to 80 per cent of the calls within 30 seconds.

3.2.9 UN E-Government Index

The development of e-government and worldwide initiatives is tracked by the United Nations Department of Economic and Social Affairs. The findings are published as an index rating the countries based on their maturity levels. The top 20 countries on the UN's e-government Index are mostly high-income nations, since they are best able to create an environment for active citizen engagement. Furthermore, the UN index itself is weighted toward a strong telecommunication infrastructure and the excellent development of human capital through education and other types of training. Both these attributes require substantial resources spent over a long period of time. Nonetheless, some developing countries are overcoming these obstacles and closing in on higher-income nations. Given the ubiquity and rapidly falling prices of mobile technology, it is likely that tapping into cellular communications could enable emerging

countries to close the e-government gap between themselves and more developed nations.

The 2016 United Nations E-government Index indicated that e-government in the Gulf Cooperation Council (GCC) countries has become a development indicator. Bahrain and the United Arab Emirates have been listed among the global leaders with very high e-government capacity, and eight other Arab countries including Jordan, Kuwait, Lebanon, Morocco, Oman, Qatar, Saudi Arabia, and Tunisia fall in the category of high e-government capacity. All of the other Arab countries have been listed with medium to low capacity for e-government. The report suggested that there is a great potential for the Arab countries to boost their e-government index performance. The report indicated as well that better strategic vision is required in order to realize the true potential of e-government in these countries.

Arab Countries E-Government Development Index (EGDI) 2016



Rank	Country
24	Bahrain
29	UAE
40	Kuwait
44	Saudi Arabia
48	Qatar
66	Oman
72	Tunisia
73	Lebanon
85	Morocco
91	Jordan
108	Egypt
118	Libya
137	Syria
141	Iraq
150	Algeria
161	Sudan
174	Yemen
176	Comoros
183	South Sudan
184	Mauritania
187	Djibourti
193	Somalia

3.3 Key Lessons Learned

Although the importance of e-government is clear, many attempts to implement it have fallen short of the anticipated outcomes. This typically happens for a single reason: the system is not sufficiently comprehensive. Some governments, fearful of doing too much and not being able to manage a full-fledged e-government system well enough, have only implemented small-scale, somewhat uncoordinated activities. Although valuable, these limited and isolated applications fail to produce the desired efficiency precisely because they are not end-to-end and do not take full advantage of the technological scale by blending databases, networks, architecture, and interfaces. In other words, many would-be large-scale e-government programs fray into a motley group of unfinished Internet sites under construction. Even though the e-government initiative may be initially inspired by innovation, modernization, cost gains, and improved relationships between residents and their government; these minimalist approaches become overly expensive and unwieldy cost drivers that satisfy no one and hence lack acceptance and usage.

The following are some of the key lessons learned from e-governments across the globe that could ensure the successful realization of the intended benefits:

➔ **Ensure clear senior leader sponsorship and strategic aims.**

Successful e-government programs depend on strong support from the very top ranks of the government.

➔ **Develop a comprehensive e-government strategy from the start.**

To make the greatest impact, a comprehensive e-government program should include four attributes: (1) end-user-driven modernization, offering individuals and businesses consistent interaction and efficiency when dealing with the government, as well as improvements designed to make customer interaction with the government less cumbersome, and with end-to-end services; (2) an approach that targets the entire portfolio of government services; (3) a cross government design that cuts across agency and organizational boundaries; and (4) an efficiency-driven program using state-of-the-art technology.

➔ **Rethink government as a service provider and focus on service modernization.**

Consider government interaction with individuals and businesses from the customer perspective, and then generate a comprehensive catalogue of end-user-focused services - prioritized by their attractiveness to the intended audience - to include in the e-government system. Top services will vary from country to country, but typically the most popular are employment opportunities, grant applications, identity card applications, vehicle registration, tax payments, and driver and business licenses. The next step is to evaluate each set of applications against these three criteria: highly attractive and easy to implement, highly attractive but difficult to implement, and less attractive and difficult to implement. Based on this analysis, the overall structure of the e-government system and the implementation schedule for specific services can be designed. In addition, government services should be revisited

regularly to ensure that the e-government system addresses the current customer needs.

➔ **Do not focus on Web services only - follow a multi-channel approach.**

The precise channels to use for specific e-government services should be tailored to the needs of the customers (based on demographics and other factors) and the business community. The possible channels include online, phone (landline and mobile), fax, e-mail, regular mail, and interactive TV, as well as onsite service desks and kiosks.

In fact, the articulation and emphasis of access channels should reflect the behaviour of the country, for example, with 80% mobile phone penetration in Algeria, but just 15% Internet usage, the e-government system in that nation must be tilted to ensure that the mobile channel is robust and operating at peak performance all the time. By contrast, the Web portal should duplicate the mobile application, but it could be a lower maintenance priority.

Similar levels of usage can be found in most Gulf Cooperation Council countries, in which the mobile phone penetration generally ranges between 150 and 200% - the United Arab Emirates has a 200% penetration, while Saudi Arabia is at 180%.

Regardless of which channels are chosen, the customer

experience should be the top priority - consistently high quality, across all channels, with a similar customer interface.

➔ **Build a solid technology platform with a set of core components across entities.**

For most e-government systems, the Web-based portal is the heart of the infrastructure - the public face for a complex variety of interconnected technology components that operate behind the scenes, which may include government data centres, government networks, as well as enterprise architecture. To keep the system up-to-date, it is important to constantly reassess the status of the technology, adding new layers as they are developed: Web 2.0 applications like peer-to-peer discussions, wikis, and social networking, as well as more the advanced integration technologies like XML, and open API. In addition, information security safeguards and privacy controls with roles and responsibilities to manage these policies must be built into the system at the technology platform level, accompanied by detailed instructions on how to implement management and functional control processes.

➔ **Define an interaction model between centralized and decentralized responsibilities.**

There should be a dual-tiered coordination and delivery system. Under this approach, the overall management of strategy, master plan, programs, design, consistency, end-to-end applications, and so forth are centralized and handled

by a dedicated e-government agency. The decentralization aspect relates to the role of individual government agencies to help design the applications and services involving their specific activities and to operate these programs, alerting the e-government unit of any problems and potential improvements. The challenge is then to create an interaction and engagement model by which to disseminate the knowledge and leverage the momentum from the e-government agency to the decentralized government bodies involved in the program. This drive should lead to a change agenda within each ministry, with top management commitment and an agenda that overcomes obstacles in establishing an e-government system as well as mobilizes the entire governmental organization with the appropriate learning and training programs.

➔ **Engage in tireless and unwavering program management.**

E-government programs fail when they are not managed diligently so that the steps are not taken to avoid such common mistakes as inadequate staffing, supplier conflicts, technical problems, project planning weaknesses, and the lack of clearly defined objectives. To avoid these problems, project management must be tireless and unwavering. Each project in an e-government system must be coordinated and monitored within nine separate dimensions that encompass everything from project initialization through to implementation and on-going maintenance.

➔ **Present success stories rapidly share some quick wins.**

Implementing an e-government program can take four years or more. As a result, quick, early successes are essential to build momentum and maintain support for the overall project.

➔ **Communicate the program and benefits of e-government.**

This phase may seem obvious, but many governments neglect it. It is vital to promote the e-government system with attractive communications and marketing materials that present the program in an appealing light. The critical goal is to excite individuals and companies and attract them to the website and other channels in the hope of creating a virtuous circle of usage and support among users and the government agencies. Both of these outcomes can mean the difference between a constantly improving e-government system that, in turn, propels greater government and economic performance, as opposed to a system that is barely noticed and never delivers the intended value or payback on the investment in cost and effort.

➔ **Build in-house capacity, and don't underestimate change management.**

E-government programs require a significant in-house organizational change in order to be successful. The project completely alters the way the government does business with residents and other governments, so that a wide-spread

shift in culture and behaviour cannot be achieved without a commitment to change management. Led by the upper tiers of the government, a change agenda must be driven throughout each ministry and agency. In addition, the technology arm of the government should evolve into a full-fledged organization, to help manage, oversee, expand, and promote the continuous evolution of the e-government program.

Such a substantial transformation can only be accomplished with the right blend of supervision commitment to change. To drive this, governments must (1) lead from the top by requiring high-level managers in the organization to champion the initiative; (2) demand a change agenda from each ministry or agency, approved by the heads of the departments; and (3) make sure that the change agendas cascade down through the ministries with the support of the appropriate learning and training programs that mobilize lower-level employees to embrace the goals of e-government.

The key aspect is that, it is almost impossible to copy one technical solution from one public sector organization to another. This is true not only on the international level, but also in the national context. Therefore, the best practice solutions in this study cannot be copied, but should be used entirely as an inspiration to develop a government's own ideas, concepts and models, keeping in mind that the development of relevant technical solutions to implement these ideas is, in most cases, only a minor issue.

3.4 TRANSFORM Strategy

From the detailed literature study conducted and by examining the UN e-government survey reports, it is amply clear that the political leadership and e-government leaders need simpler and effective tools for visualizing and conveying strategies. These roadblocks made us study the common phenomenon around us, which people are familiar with that resembles the issues and challenges faced by e-government projects, i.e. resistance. Different analogies were considered and it was finally found that rocket propulsion is a concept that most people are fairly familiar with. Opposing forces act on a rocket, which are called resistance which a rocket needs to overcome through the appropriate thrust in order to reach its goal – of taking off.

3.4.1 Rocket Analogy to E-Government Projects

A good analogy which is understood by the key decision makers can convey more information than any lengthy description of text. However, the analogy, even though, it cannot replace the formal definition of the strategy, on the other hand, it can provide valuable abstraction in a way that can be easily conveyed. Primarily the selected analogy should be able to convey maximum details about the project being considered through a graphical medium. This would save valuable time and enable a better coordination as it brings a lot of clarity and reduces ambiguity to the program.

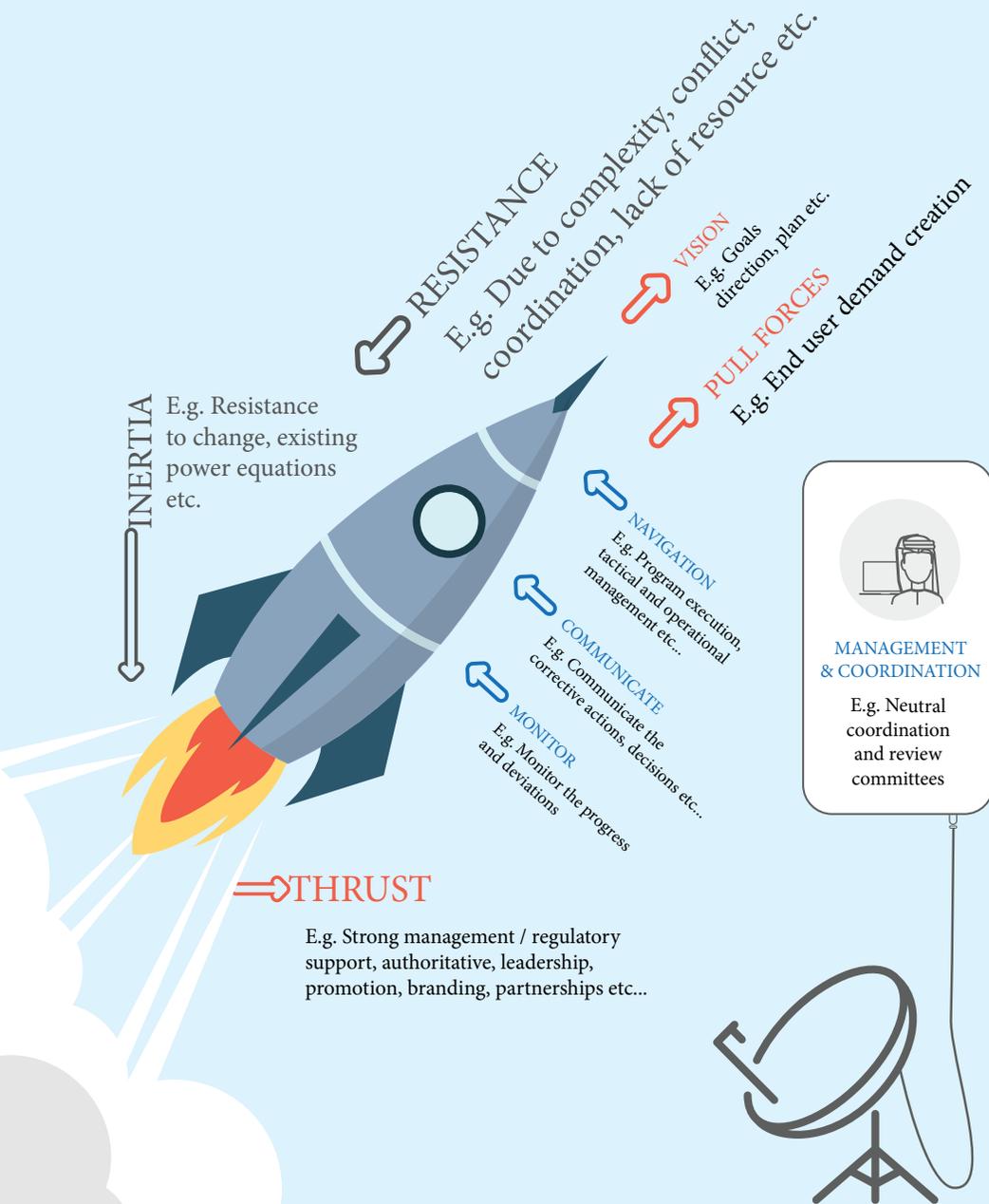


Figure 9: Rocket Analogy

Looking at the diagram, we can identify the forces that act on the rocket. Inertia is an opposing force that we most commonly encounter in projects, which oppose any changes. One needs to apply a heavy thrust in order to overcome the inertia till the rocket (project) gains significant momentum. Once in motion (execution), the rocket faces continuous opposing forces, which although not as strong as the inertia, can slow down the projects or produce total failure, if not handled properly. These resistances can be in the form of coordination issues, technical issues, and a lack of standards etc. A rocket applies thrust to overcome these opposing forces. This thrust can come as a push which means from the management or pull from the customer side. During the course of flight, there is a need to continuously monitor the flight path to detect any deviations, which once identified, need to be communicated to the rocket navigation system to take controlling actions.

3.4.2 The TRANSFORM Model

From the analogy described above, we can derive a model that maps the e-government domain artefacts and problem statements. This model named as Thrust, Resistance And Navigation Strategy Form or in short as TRANSFORM is illustrated in the following diagram.

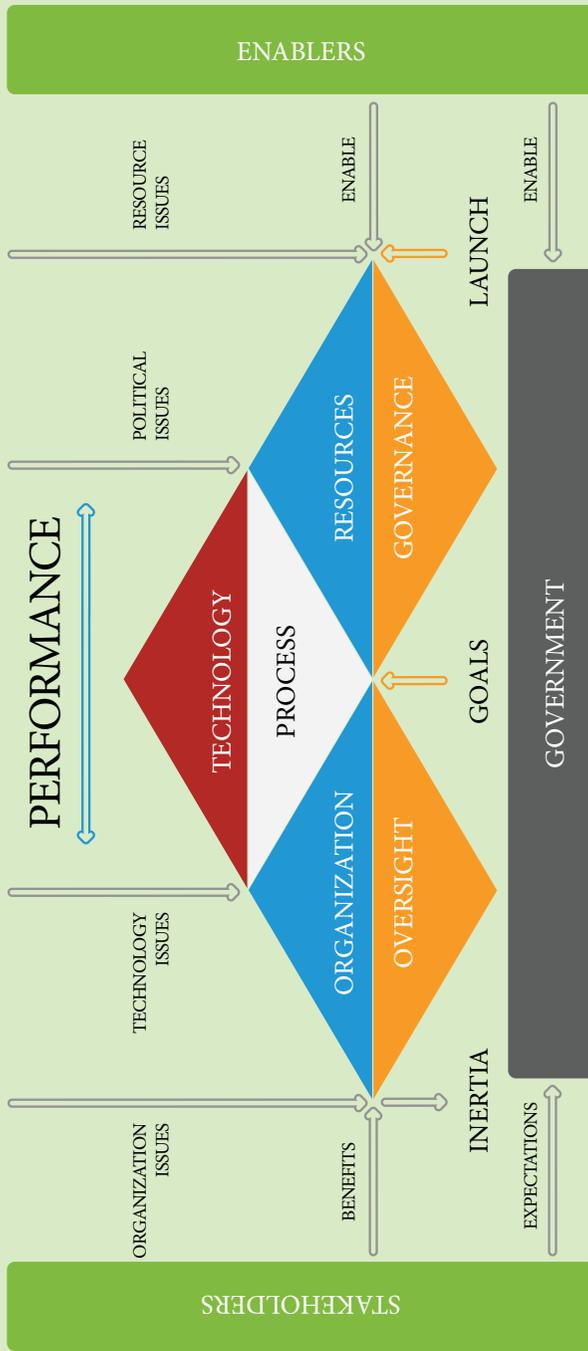


Figure 10: TRANSFORM Model

This graphical visualization of the strategy would be beneficial to the decision makers. It is more convenient for politicians who are normally non-technical. It is always easier for them to handle graphical representations than to study huge tables, lengthy texts, etc. Furthermore, a strategic framework gives a simplified, yet a comprehensive conceptualization of what the e-government strategy is all about. This is particularly important during discussions about e-government initiatives among stakeholders. Whenever the need arises to consult the strategy, it might just be satisfactory to consult the framework first. In case further details are required, then the complete strategy is always available. This can, in many cases, save the time and effort of delving into the full text of the strategy.

3.4.3 Stakeholders

An e-government project is meant to deliver benefits to its various stakeholders, whether they be internal or external, or direct and indirect stakeholders. A stakeholder would be an individual or an organization that is impacted or associated with the said e-government project. In such a case, it becomes important to conduct a stakeholder consultation at the beginning, while conceptualizing the project, in order to understand their needs/ services from the government. Similarly, the needs out of the project for the internal stakeholders should also be consulted in the beginning.

3.4.4 Expectations

All projects are intended to meet the needs of their stakeholders, first; therefore, it becomes imperative to assess the project to meet their expectations before moving forward. The TRANSFORM framework model emphasizes listing the expectation indicators, which are measurable from the various stakeholders' perspectives. These expectations may differ even for similar category of project (e.g. G2C Rural or Urban, G2B), depending on the country and its geographical area of implementation.

3.4.5 Project Benefits

These expectations are then taken into consideration for the conceptualization of the service requirement and, accordingly, built into the e-government project development in order to deliver the benefits to its stakeholders. The benefits are the front end component of the project, which are visible to the stakeholders, and could be in terms of impact, or return on investment (ROI).

A lack of the perceived benefits can result in a lack of motivation for the citizens to come forward and avail themselves of the e-government services. Hence, it is important to initially focus on the initiatives that greatly enhance the convenience as well as deliver benefits to the people. Such initiatives should be selected based on their large coverage and their impact. Such applications can generate a pull factor, generated by the demand from the people.

3.4.6 Performance Indicators

The project, in terms of the benefits delivered to the stakeholders, can be measured by specific performance indicators. These indicators are required to be listed and prioritized based on their importance to the project. Each indicator could require a different approach and methodology for measurement. The point of concern is really to identify the performance indicators, which are specific to the project perspective, and which can be completed always taking the set of constraints into consideration.

3.4.7 Enablers

The goals are driven by 'enablers' at the back-end, which would indirectly be responsible for delivering the said outputs. These enablers push the project to deliver results, which are passed on to the stakeholders. The enablers would not yield direct results themselves. There could be two approaches for identifying the enablers - one set of enablers is linked to each of the performance indicators; the second, is to list the broad set of enablers which drive the project to deliver the results. These sets in turn are further divided into sub-attributes, which are then measured on a particular scale. The TRANSFORM framework illustrates the second approach and lists the key set of enabler indicators, which would further be measured through specific sub-attributes.

3.4.8 Resistance

Some of the major resistances or challenges faced by e-government projects are described below:

3.4.8.1 Inertia

The public administration management and staff's resistance to any innovation can impede, impair or prevent the necessary redesign of the organization and the processes that are required to deliver an effective e-government. Such inflexibility can set up barriers to the creation and delivery of efficient and effective e-government services, which could meet the changing needs of both citizens and businesses. The factors that contribute to this inertia include inadequate staff skills; a lack of training and investment in staff both in terms of ICTs and change management competencies required for innovation in e-government; a fear of change; risk aversion by government staff, which may be exacerbated by the frequent poor track record of e-government initiatives, which have included high-profile failed projects that have caused significant problems for both citizens and companies; fears of increased liability risks if sharing networked resources across different public services; as well as a limited sharing and learning of experiences and lessons from good practice.

3.4.8.2 Organization Issues

Often government ICT projects are also quite complex because

several organizations are involved that are more or less autonomous. One can think of a number of organizations that have joined forces in an ICT project because their business processes were related so required the exchange of information. In these cases, central steering of the project is difficult or sometimes even impossible. Since organizations tend to act primarily from their own set goals, their contribution to and acceptance of the ICT project may depend largely on how the ICT project can serve these specific goals.

Another aspect of organizational complexity is because of the strong interconnection between ICT and the given organization. An ICT project, generally, implies organizational change and, conversely, this organizational change can have a significant impact on the ICT landscape.

The emerging forms of e-government service delivery and the varied ways of working often cross traditional government jurisdictions and administrative and departmental boundaries, and, as well, have the potential to overcome geographic distance. Variations in legal, regulatory and administrative regimes on different sides of these boundaries can inhibit and block the flow of information and services through the new networked governance channels at the national, regional and local levels. Thus, effective coordination across regions and departments is particularly important because the responsibility for directing public administration activity is frequently fragmented and shared across multiple levels. There also can be an adverse distance between the government and other stakeholders which can further block effective nation-wide e-government.

Often one can find multiple e-government initiatives that seem to achieve similar outcomes. Eventually these initiatives tend to compete with each other to gain prominence. This kind of unhealthy competition and the largely overlapping initiatives could result in wastage of resources and time, as well as in redundant initiatives. This normally arises from the lack of an overall vision and a roadmap for the nation so that each agency is allowed to define e-government strategies that are not necessarily aligned with common national goals.

3.4.8.3 Technical Issues

There is an inherent mismatch in flexibility between ICT systems and political and organizational processes. The latter are dynamic and flexible by nature; however, once a decision has been taken to develop a particular ICT system and the project is underway, it is difficult to change the project. Such changes are not impossible, but have their price in terms of time and budget overruns. Another complicating technical factor is that ICT systems often have to be connected to other systems already in operation. Compatibility between ICT systems - already a major issue within a single organization—becomes, especially, challenging where a number of organizations are involved. The problems that arise when collating data from two or more organizations, if the data entries do not agree with each other, (conversion problems) are often underestimated.

Further to this, advances in ICT succeed each other at a daunting pace. This tends to make expertise and know-how quickly become

obsolete as new up and coming techniques that become available during the project place the chosen strategy in a new light.

Issues of trust, and the lack of it, have always been a strong ingredient in shaping the structures and practices of governance. It is, therefore, not surprising that a concern about trust in e-government is a crucial element in the take-up and effectiveness of e-government services. At the heart of these concerns is the security of the data collected on individuals and identity theft issues. To help overcome trust concerns, trustworthy mechanisms, in which there is a wide confidence, need to be developed to protect citizens from the unauthorized electronic disclosure of personal information, which could include the transfer of such data between public bodies or between public and private organizations.

E-government systems and services frequently also fail or perform poorly because of inadequate design and poor technical interoperability. Difficulties caused by inappropriate user interfaces for e-government systems can seriously hamper relations between public agencies, citizens and businesses. Such poor usability features can sabotage even potentially successful services and discourage those who have experienced them from trying other e-government opportunities. As noted above, interoperability issues, including technical interoperability play a significant role in an integrated e-government. Incompatibilities in hardware, software or networking infrastructures within and between public agencies can cause significant problems, particularly, in terms of providing integrated services.

3.4.8.4 Political Issues

Political decision makers tend to believe that ICT is the ideal solution for any policy problem. Senior civil servants, ministers and members of parliament often do not fully comprehend what ICT can do and, more importantly, what it cannot do. A minister who takes decisions without seeking adequate advice runs the risk that the project will be unrealistic from the start. Also, it is not uncommon for a project deadline to become the outcome of a political debate or the statement of an ambition, instead of an underpinning and realistic planning result. Unrealistic timing can lead to serious trouble with projects.

Social and economic divides - demarcated by wealth, age, gender, disability, language, culture, geographical location, size of business and other factors can mean e-government resources are used in very different ways (or not used at all) by various individuals, groups and organizations. These divisions range from users at the ends of electronic 'pipelines' who may not know that there is a 'tap', how to find it or how to turn it on to those with much expertise who are conversant in interacting in sophisticated ways either as providers or as consumers of digital content.

It is important to address all the accessibility gaps both in terms of access to technology and in the levels of ICT skill as well as to ensure such networked services meet the greatly varying range of perceptions, knowledge and capacities among the actual and potential users. Without a more nuanced understanding of user needs and choices, the uptake of e-government will remain limited and the potential benefits will not be realized.

3.4.8.5 Resource Issues

The costs of developing, implementing and maintaining e-government (such as the costs of software, hardware and training for government officials) can all be resistances to adopting e-government. Related to this issue are the difficulties of being able to measure the cost/benefits of e-government initiatives. Although, some benefits can be seen in clearly measurable terms (e.g. staff numbers and reductions in cost overhead), many cannot be defined with confidence in a similar way as they are too qualitative, intangible or unpredictably set in the future (e.g. improved quality of service, new services, responsiveness to citizen needs or avoidance of costs that would have been incurred using non-digital channels).

The difficulties in calculating substantive tangible benefits to offset clear and often apparently high costs can lead to the financial tap to e-government services being tightened or turned off. This can severely hamper the speed and scope of any e-government progress.

Inadequate skilled resources can also become a major bottleneck in e-government projects which leverage advanced ICTs. e-government strategies should first address the need for adequate manpower and the training needs.

3.4.9 Thrust

The major thrust areas of e-government are described below:

3.4.9.1 Governance

Often a lack of authority and leadership has been attributed to many failed projects. As the e-government initiatives span across various administrative boundaries, a knowledgeable and empowered steering committee or leadership must be in place that can make the necessary decisions and enforce them.

As has previously been discussed, many of the resistances stem from the lack of common standards, agreed upon procedures and methodologies. These include legal and regulatory policies and guidelines in addition to technical and operational standards. The enforcement of these policies would ensure the proper alignment of independent initiatives and thus enable interoperability between departments.

3.4.9.2 Goals

Goals are defined by the government to meet the stakeholders' expectations. These goals are both qualitative and quantitative in nature. We may follow the SMART (Specific, Measurable, Achievable, Relevant, Time-bound) approach to defining goals. The clear definition of the e-government vision and goals would help the departments to align their strategies with the shared vision. This should include strategic outcomes of the projects in quantifiable terms. A periodic review of the initiatives can assess the progress made towards achieving the defined goals.

3.4.9.3 Launch

Inertia is a major aspect any major project so it must be addressed in the initial stages. If enough thrust is not provided at the start of the project; the project momentum will eventually yield to the inert forces so it will fail to take off. Hence, it is very important to have the appropriate launch for the projects. The launch can involve various activities such as marketing, communication/publicity, a launch event, branding and the endorsement by political leadership.

Marketing and branding are very important aspects by which to gain wide respect and recognition for the e-government initiatives. Generally, e-government initiatives do not consider these as important. However, we can see that corporate and business enterprises do successfully use branding and marketing strategies to get the products and services to the people. Therefore, there is a great need for e-government projects to be branded and promoted in order to gain wide visibility, recognition and demand.

3.4.9.4 Supervision

The complexities of the different dimensions of e-government projects underscore the importance of having an effective and active overseer – for Monitoring and Evaluation (M&E), which is a framework to measure the output, outcome and the overall impact to provide information for informed decision making. The M&E framework would thus:

- ➔ Provide a common institutional mechanism for monitoring, reporting, controlling and disseminating information for both physical and financial progress, outputs and outcomes.
- ➔ Help in the identification and resolution of delays/ risks on a timely basis.
- ➔ Measure the impact-assessment post program implementation;
- ➔ Generate inputs for policy making and facilitate better program planning, management as well as improve program performance monitoring and evaluation work together in unison, but are actually distinct functions serving varied purposes. They are complementary functions performed sequentially in a program.

However, both Monitoring and Evaluation focus on delivering.

- **Efficiency:** Measure whether output is desirable with the inputs provided.
- **Effectiveness:** Determine whether the program has achieved the desired goals and objectives.
- **Impact:** Determine whether there has been a measurable improvement post-implementation

Approach for Designing and Implementing M&E

M&E forms an integral part of an overall program and, hence, it should be tightly integrated with the overall program approach. The essentials of the approach are:

- Define objectives
- Define framework
- Identify components and indicators (quantitative and qualitative) to be tracked
- Process for implementation
- Select requisite data points
- Collect data
- Data analysis
- Reporting and feedback
- Institutional framework

3.4.10 Navigation (Project Management)

Finally, let's define the navigation strategy for our framework. As illustrated in the diagram, (WHICH ONE?) an e-government project is an ecosystem of resources, processes and technologies. These three components must work in close coordination in the implementation of any project. To ensure the alignment with common goals and to meet the defined performance criteria, it is a common practice to have an independent review committee (supervisory body - overseer), which periodically monitors and reviews the progress of each project. These observations are then communicated to the project leadership so that they can enact specific controls to bring corrections and re-alignment.

3.5 Conclusion

Clearly, an e-government initiative demands a full, long-term commitment and will encounter many obstacles and challenges along the way, but it is well worth undertaking. In fact, more and more governments will no longer have the option to lag behind because automating transaction and information activities both within and outside the country will be so commonplace that an e-government system will be required to maintain efficiency levels, economic performance, policy implementation and, last but not least, attain a place in a globalized automated world.

4

STRATEGY EXECUTION AND OPERATIONAL MODELS

4. STRATEGY EXECUTION AND OPERATIONAL MODELS

E-government transformation is a long term endeavour, which is seldom impacted by any short term technology trends. This section enlists the overall planning, working models and operational details of the strategic integration of any e-government transformation within the context of a national identification program. It also brings forward the experiential makeover of all the interactions and transactions between the government, agencies, services and the citizen. It also outlines the details of the delights of the citizens in a completely digital government.

4.1 Guiding Principles

The following are the important guiding principles and characteristics of a transformed government:

➔ **Citizen-centricity:** This refers to viewing the government from outside-in, i.e. understanding the requirements and the expectations of citizens becomes the pre-eminent guiding principle for all government policies, programs and services. In short, this represents the service-dominant logic which requires the government to operate as one enterprise and organize around its citizen demands and requirements. Aside from the citizens per se, other government constituents, such as businesses and civil organizations are captured

as well in the social inclusion dimension, which will be described later.

➔ **Common infrastructure and interoperability:** This refers to the use of standards and best practices across governments so as to encourage and enable the sharing of information in a seamless manner. Interoperability is the ability of organizations to share information and knowledge within and across organizational boundaries. The underlying foundation for effective interoperability comes from a standardized common infrastructure.

➔ **Collaborative services and business operations:** A connected e-government requires all the necessary ministries and agencies to collaborate. It is not difficult to uncover actual success stories about integration and interoperability at the technology level. However, to collaborate at the level of business services and functions needs political will. This is because collaboration at this level leads to shallower 'stovepipes', the elimination of redundant or overlapping services and the discovery of common and shared services, which in turn lead to a loss of authority and more control for others.

➔ **Public sector governance:** This refers to the decision rights and the accountability framework that is required to implement all of the other strategies for a connected government. Good governance is a non-negotiable factor in the success of the connected e-government, more so for countries that have multiple levels of governments (i.e., federal / central; state / provincial; and town / city) where various levels could be administered by different political parties.

➔ **Networked organizational model:** This refers to the need to accommodate new organizational models wherein the enterprise (in this context the whole of government) is a network of relatively autonomous ministries and agencies working in a coherent manner in order to deliver value to both its citizens and businesses. This makes the entire government a networked virtual organization (NVO) that operates seamlessly towards a common mission.

➔ **Social inclusion:** This refers to the ability of governments to move beyond the horizontal and vertical integration of government service delivery to engage their citizens and businesses at relevant points in the policy and decision making processes. E-democracy and social inclusion ensures that the delivery of government services is not a one-way interchange. Innovative ways of using technology to facilitate constituent participation and to build a consultative approach is an imperative for the success of a connected government.

➔ **Transparent and open government:** This refers to the political doctrine, which holds that the business of government and state administration should be open at all levels for effective public scrutiny and supervision. In its broadest construction, it opposes the reason of state and national security considerations, which have tended to legitimize extensive state secrecy.

4.2 Issues & Challenges

E-government brings all-encompassing changes, which in turn bring in a whole lot of challenges.

➔ **Ownership** – The lack of national ownership results in the absence of a cohesive e-government strategy, and little consideration for the local context and cultural and social issues. The reasons are: a reliance on external experts, which means ignoring the main stakeholders in e-government planning, which then causes a lack of ownership, and a dominance of politics and self-interest.

➔ **Leadership** – A lack of leadership at different levels of government, especially, sustained political leadership, and a lack of commitment from the top management and senior officials, which causes resource misallocation and a negative message to other groups.

➔ **Vision and Strategy** – The absence of a long-term vision and a cohesive implementation strategy results in the lack of guidance and connection between ends and means, uncoordinated and isolated projects, and dispersed responsibilities due to multiple ownership.

➔ **Institutional Capability**- Weak or absent institutions for e-government policy and coordination, with low administrative capacity and management liabilities within the government, which can result in a lack of coordination among e-government projects, and a lack of collaboration between different functions and levels of government and between the public and private sectors. Also, poor project and program management, weakness of controls, ineffective procurement and change management spells disaster.

➔ **Design Versus Reality** - Unrealistic expectations and a poor understanding of the needs of the people result in a poor design, which does not match the local environment including the culture,

values and needs. This is caused by the lack of input from local stakeholders that occurs when foreign donors and consultants drive the e-government efforts.

➔ **Capacity and Awareness** - A huge gap exists between the capacities required for e-government and the capacities present in most developing countries, with a shortage of qualified personnel in government and a lack of awareness among officials and citizens. Also the gaps exist between the educated and uneducated, the rich and poor; all of which results in negative attitudes to e-government, a resistance to change, and a biased provision of E-services.

➔ **Dependence on External Assistance** – Due to limited financial and human resources, many e-government initiatives in developing countries are dependent on the aid agencies, vendors and consultants, which, needless to say makes them particularly vulnerable when the outside funding ends. When donors work with different agencies, isolation, fragmentation and a duplication of applications may be reinforced.

4.3 E-governance Transformation Contexts

E-governance exists in different contexts. Depending on the context, the meaning of e-government is seen from a different perspective. Each of these contexts needs to be addressed differently as the issues and challenges vary from context to context.

4.3.1 G2C and B2C Context: Citizen Services

It goes without saying, that with the rise of digital channels, customer service is changing. The world is becoming more connected; not just between individuals but also between devices. In this environment, the citizens determine how they want to be served. Many individuals and businesses now 'live' seamlessly on the Internet so want to access government services electronically.

To meet these trends, governments can deliver real-time access to services, which increase the opportunities for citizens to serve themselves, reduce turnaround times and the resources required to deal with routine requests. ICT solutions including mobile applications, contact centres, conferencing and collaboration solutions can all help deliver these outcomes. As governments become more citizen-centric, they may need to create new delivery models to meet people's needs and to increase customer satisfaction.

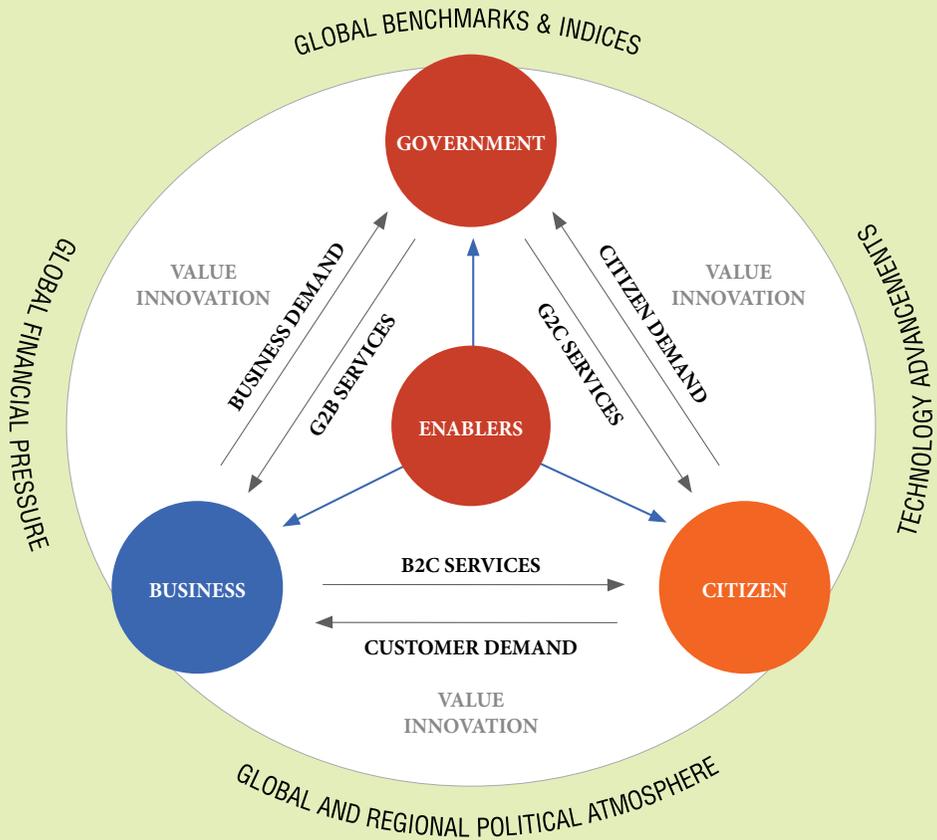


Figure 11: E-Government Transformation Context

4.3.2 G2G and G2B Context: Integration & Interoperability

The G2B domain focuses on the interaction between government and businesses via a computer mediated environment. One of the earliest examples of G2B interaction is via a electronic data interchange (EDI), which represents a standardized method for sharing documents. EDI technology is used for transactions such as the online procurement of products by both businesses and governments, with benefits such as reduced transaction costs and increased operational efficiency.

Businesses participate in e-government via two main tasks: (1) **Search-oriented tasks**: seeking information for their business, and (2) **Transaction-oriented tasks**: completing various tasks online. In addition to the above two levels of interaction, we propose that businesses have a third task level of interaction with government - network-oriented tasks. This third level is based on the knowledge that businesses are motivated by the economic, market, and the technology related factors that allow them to participate in strategic alliances for e-government procurement.

This third level refers to the use of an e-government platform where businesses can establish online networks and partnerships with suppliers, customers, and even competitors. Examples of search-oriented B2G participation include looking for contact information about the government agency, identifying services the agency provides, and searching for job and contract opportunities at that government agency. Transaction-oriented participation involves

the business, completing a task such as licensing, tax filing, or grant submission at the e-government portal.

G2B implementation is easier than G2C. It can also be outsourced because of fee-earning potential. Here lies the potential for quick wins.

4.3.3 Enterprise Context: Security, Efficiency & Accountability

In the enterprise context, we can see the application of e-government and electronic identity systems especially in the following context:

➔ **Encryption and Digital Signature Services:** Security and accountability are the two main aspects that are critical in building trust in e-government; at the enterprise level, the electronic identity technologies along with PKI can be used to secure transactions with encryption and digital signatures. With the advent of electronic identification technologies, enterprises do not need to build redundant and expensive infrastructure to avail themselves of these advanced capabilities.

➔ **Enterprise Logical Access Control (LAC):** Logical access control modernization involves integrating an Enterprise's IT resources at the enterprise level, in order to control access in a streamlined and consistent manner. Modernized logical access control standardizes the use of the electronic identity card (e-Identity) as the common means to validate the identity of a user and grant them access to networks and information systems.

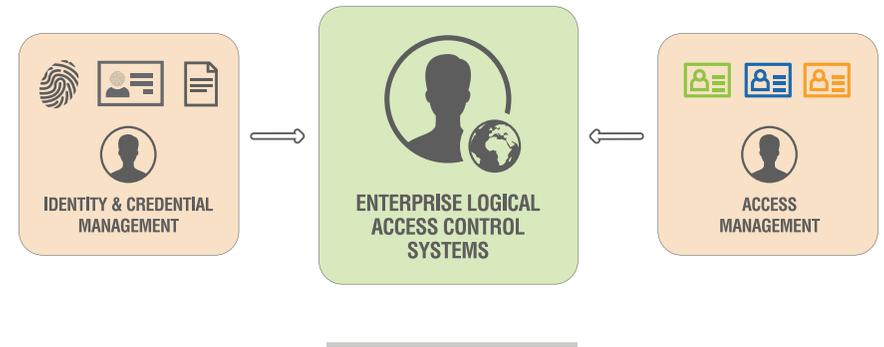


Figure 12: Enterprise Logical Access Control Systems

➔ **Enterprise Physical Access Control (PAC):** This involves integrating Physical Access Control Systems (PACS) at the enterprise level, which help an agency achieve cost savings and efficiencies while preserving local access control decisions. Modernized PACS leverage user identity and credential data from authoritative sources and are supported by enterprise resource, privilege, and policy management processes. PACS modernization also includes the use of the e-Identity card in order to gain physical access to an enterprise's controlled facility, in accordance with security best practices.

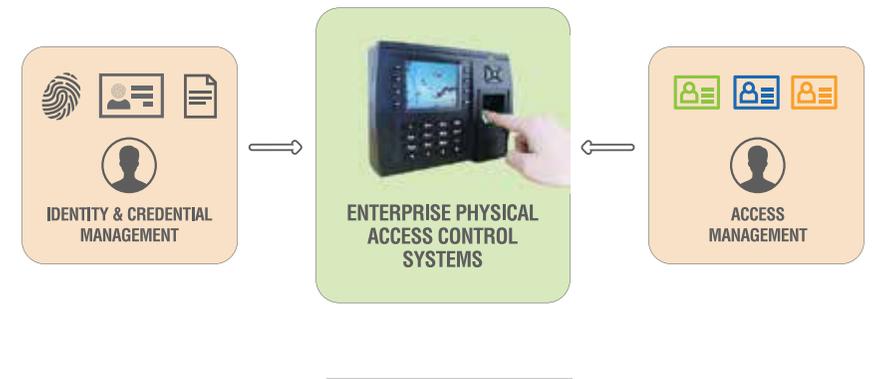


Figure 13: Enterprise Physical Access Control Systems

➔ **Enterprise Physical Access Control (PAC):** This involves integrating Physical Access Control Systems (PACS) at the enterprise level, which help an agency achieve cost savings and efficiencies while preserving local access control decisions. Modernized PACS leverage user identity and credential data from authoritative sources and are supported by enterprise resource, privilege, and policy management processes. PACS modernization also includes the use of the e-Identity card in order to gain physical access to an enterprise's controlled facility, in accordance with security best practices.

4.4 Towards Citizen-Centric & Citizen Delight

Citizen-centred service considers citizens' needs at every stage of the service design and delivery process; that is, citizens' needs become the organizing principle around which the public interest is determined and the service delivery is planned. Some of the aspects of citizen-centric e-government include:

➔ **Customer Centric Design:** Customers are categorized into segments that have different needs and expectations in terms of information, service standards and offerings. Examples could be ethnicity, citizen status, special needs etc.

➔ **Value Added Services:** Customers' needs are reflected in life event bundles. These bundles group related services from multiple entities, and are mutually exclusive in terms of

services required.

➔ **One Stop Shop:** Getting information and being able to apply for services is done in one place without having to visit multiple locations, websites or calling different toll free numbers.

➔ **Multi-Channel Access:** Service information, application and delivery are enabled through multiple channels. These could include citizen service centres, online platforms, contact centre, mobile/sms, kiosks and others.

➔ **Integrated Government:** Government entities work in collaboration to provide integrated services across multiple ministries, reduce duplication, and drive efficiencies across the entire government. General information and transactions are handled by one service entity, whereas more complex cases are handled by their respective departments.

The following trends will enable future citizen services:

- New means of assuring privacy and integrity (PKI & Digital Signature).
- Rapid expansion of digital, personalized services (Identity Management).
- Expansion of channels (mobile and social media).
- Service offering integration with citizen life events.
- Public private partnership and multiparty services.
- Increasing citizen engagement in service innovation.

4.5 Key Operational Aspects

The innovative use of ICT can drive the development of new service delivery models. In this context, organizations can implement cloud and manage service solutions to better meet citizens' needs.

It is now easier for organizations to outsource complex functions thus allowing them to re-focus on their core business. Managed service arrangements give governments the ability to work with service providers for the end-to-end management of non-core functions that lead to improved delivery and predictable on-going costs.

E-government has to move on from being a disruptive change driven by central or specialist groups to becoming intrinsic to the way governments will work in the future. Countries have identified a number of challenges that governments currently need to address in order for e-governments to deliver on their promise of a better government.

Many countries have realized that better government is simply more user-focused e-government where services and interests are aligned with citizen and business needs. In bringing this vision of government closer to users, governments may need to re-think government organizational structures and processes in order to better meet individual needs and realize efficiency at for the entire government. At the same time, user-focused e-government will be required to ensure that users are able to interact with government at their convenience regardless of the channel they use.

4.5.1 Infrastructure

Infrastructure is probably the most obvious and tangible dimension of e-government. As e-government is characterized by procedures and services taking place between administrations on the one side and citizens or businesses (or other administrative entities) on the other, technical infrastructure is needed to carry information and services. This characteristic distinguishes e-government from earlier forms of interaction with an administration. e-government provision is not linked to a specific technology, but rather to any electronic means that citizens and businesses use to send and receive: voice, data, and images via the Internet, such as personal computers, laptops, personal digital assistant devices (PDAs), as well as mobile or fixed line telephony.

The effectiveness of e-government services in reaching citizens and businesses depends greatly on the availability of ICT infrastructure. Therefore, it is relevant for decision makers to evaluate the status and development of the ICT infrastructure in their own countries and plan e-government projects accordingly. To assess the level of access to ICT infrastructure, decision makers can use data collected from telecommunication incumbents and Internet providers via individual, business and household surveys. A well-informed analysis would also profit from knowledge of citizens' affordability of access to ICTs, looking at tariffs for certain services, in comparison to per capita income levels. Finally, the infrastructure dimension also extends to the energy sector, as access to electricity is a precondition for a functioning ICT infrastructure.

4.5.2 Policy

A policy is a deliberate plan of action to guide decisions and to achieve rational outcomes. Commonly, governments develop and implement policies to address basic socio-economic issues that are expressed by laws, budgetary actions, international agreements, declarations, contracts or campaigns. Different types of policies shape the e-government environment. Trade regulations control the import and export of ICT goods, which affect the provision of services. Policies that protect the local ICT industries, including tariff barriers, alter the movement and price of goods on the market. Similarly, anti-trust regulations and market liberalization strategies, enforced by telecommunication regulatory authorities, have enabled: the conditions for greater competition in the sector, the introduction of new technologies and services, and better prices for consumers. Likewise, the inclusion of universal service obligations in the licenses of telecommunication incumbents or Internet providers has promoted access to the ICT infrastructure in the least served areas, such as the rural and low income communities.

The policies protecting the critical information infrastructure also shape the e-government environment. Cyber-security policies - the protection of an e-government infrastructure against failures and attacks from inside the system, as well as from outside, are essential once a country heavily relies on e-government services. Protective measures are particularly necessary for the provision of e-business or whenever sensitive financial or personal data is being transferred electronically.

Protecting the privacy of individual users is also crucial to order to ensure that citizens trust in the new communication technologies. Accordingly, the laws and regulations regarding digital identification, digital signatures, e-payment and data protection are highly relevant, and are thus shaping the environment of e-government. While e-government policies depend strongly on the vision of the decision makers, their success requires for such visions to be formulated, expressed, shared and discussed with all the relevant stakeholders to improve ownership and ease the implementation. When policies fail to be implemented properly, the gap between plans, actions and expected outcomes grows, which results in citizen dissatisfaction.

4.5.3 Governance

Governance, that is, the performance of public administration, is the penultimate factor for the success of any e-government initiatives. The World Bank defines governance as the exercise of political authority and the use of institutional resources to manage society's problems and affairs. The optimum performance an administration can strive for is to produce a "worthwhile pattern of good results, while avoiding an undesirable pattern of bad circumstances". Therefore, to achieve good governance, different factors need to be balanced, including costs, freedom of the individual vs. the common good, local, national or global interests, as well as short and long term gains versus losses. The negotiation of these factors could lead to varying results and performances, as places and times change. Despite these divergences, there is a general consent on the minimum requirements for the good performance of a national administration. Commonly, it is recognized that a government performs well if

it, at least, does not abuse its power, is not corrupt, and follows the due processes of law, which includes a division between the executive, legislative and judicial powers, as well as freedom of the press. This paradigm is often also called “good governance” in development literature. Further, the success of e-government initiatives also depends on defining back-office workflows within the administration and on digitalizing and re-engineering those workflows. Since citizens do not usually know the processes taking place within an administration, they judge its performance based on their personal experiences, and draw their conclusions about the quality of governance according to the time it takes to complete standard procedures such as registering a car, and their liability and how consistent the process is.

4.5.4 Outreach

“Outreach” is the dimension of e-government most prominently perceived and experienced by end users, namely companies and citizens. It is often referred to as the ‘horizontal integration’ of public services, as it brings together the various service offerings to the end-users. One aspect of outreach is the supply of information and services by governments. A government’s communication with and supply of information to businesses and citizens varies in intensity. Some administrations provide static information on web pages; others offer services online; and some others offer electronic consultation and participation. The European Union (EU), for example, practices online consultations with its citizens. It applies e-government in order to overcome long distance, language barriers and the perceived democratic deficit of the institutions of the Union.

Service oriented e-government initiatives tend to bundle different services according to a combination that an end-user would perceive as a logical unit for their situation for a one-stop-government. For instance, the government of Singapore is working on the development of an even more user-friendly government portal. To this end, the provision of information in the front end should be improved; information should be presented in a better and more intuitive “look-and-feel” way, and it would provide better search engines, for different types of media. Creating a one-stop government interface is a major challenge for national e-government efforts. The services to be integrated might represent numerous fragmented processes, which would require the involvement of a diverse number of stakeholders.

E-government activities are also affected by the demand forces that emanate from the particular needs and characteristics of citizens and businesses, such as education, ICT literacy, and other life circumstances. Many e-government applications consist of text and are Internet based, which thus require users to have at least a basic computer literacy and, if they do not rely on agencies in telecentres or other service providers, they require the ability to read and write. Therefore, it is crucial for the success of an e-government project to understand the capability of the citizens that the initiative is targeting.

This dimension also covers outreach between national governments. Peer-to-peer learning, for instance, can be very helpful. Moreover, challenges such as for cyber-security and solving cyber-crimes are cross border issues that should be dealt with in a coordinated

manner. Accordingly, a country's engaging in global and regional forums concerning e-government can improve their e-government environment.

4.6 The Role of Federal Enterprise Architecture

According to Haiyan Qian, the former Director of the Division for Public Administration and Development Management, United Nations Department of Economic and Social Affairs (UNDESA), "enterprise architecture is an effective strategic planning tool for governments by facilitating the creation of linkages and improving interoperability among government agencies, benefiting both internal operational processes as well as improved public service delivery to citizens."

Moving to a connected government requires a holistic and coherent framework, which cannot be achieved by piecemeal approaches and mechanisms. Such a framework recognizes the integrated presence of e-government both as an internal driver of transformation within the public sector and an external driver of better governance.

Typically, governments, being the largest of all organizations, are characterized by complex federated structures where individual government organizations work in their respective silos. Often, this leads to fragmented business processes and duplicated systems and technologies, which create obstacles in cross agency interoperability. Government-wide architecture thus facilitates end-to-end business

processes, standard technologies, a rationalized data structure and modularized e-services that can be assembled as required to deliver eservices. The following diagram illustrates the result of an enterprise architecture maturity level study conducted by the UN on some of the leading countries.

EA influences the development, the design and the capacity of a government's offerings of public services. By definition, connected governance is the current trend of the provision of electronic and mobile public services, in which public institutions share common objectives across organizational boundaries, as opposed to different government ministries independently supporting autonomous portals.

Connected governance also poses new requirements for governments, such as cross-organizational connectivity, as well as a back-office to front-office integration - all issues, which are addressed by effective EA. Therefore, the presence of EA is a precondition for the successful implementation of a connected government.

DIMENSIONS	UAE	AUSTRALIA	JORDAN	NEW ZEALANDS	AUDI ARABIAS	OUTH KOREA
CITIZEN CENTRICITY	MARGINAL	LOCALIZED	DEFINED	DEFINED	NONE	INSTITUTIONALIZED
COMMON INFRASTRUCTURE & INTEROPERABILITY	LOCALIZED	DEFINED	DEFINED	INSTITUTIONALIZED	LOCALIZED	INSTITUTIONALIZED
COLLABORATIVE SERVICE & BUSINESS OPERATIONS	MARGINAL	DEFINED	DEFINED	INSTITUTIONALIZED	MARGINAL	INSTITUTIONALIZED
PUBLIC SECTOR GOVERNANCE	MARGINAL	LOCALIZED	DEFINED	LOCALIZED	NONE	INSTITUTIONALIZED
NETWORKED ORGANIZATIONAL MODEL	NONE	LOCALIZED	DEFINED	INSTITUTIONALIZED	LOCALIZED	DEFINED
SOCIAL INCLUSION	NONE	MARGINAL	MARGINAL	DEFINED	MARGINAL	LOCALIZED
TRANSPARENT & OPEN GOVERNMENT	NONE	MARGINAL	MARGINAL	LOCALIZED	NONE	LOCALIZED

Figure 14: Enterprise Architecture Maturity Level - Comparison

As an ICT management and planning tool, government EA represents a business-driven approach to ICT management that emphasizes interoperability in order to achieve a connected government and governance. EA with cross-national interoperability is indispensable in the move towards connected government/governance.

A country with a strong e-government maturity that lacks an effective EA program can perhaps embark on a strategic mid-to-long term approach to implement EA, as an effective enabler to achieve its development goals, which include the effective delivery of more efficient, transparent and accountable public services.

4.7 Realization Roadmap

The key instrument for strategy implementation is the catalogue of prioritized projects. This periodically updated tool contains the measures that must be implemented in a coordinated manner within the framework of the e-government strategy. The key aspects of developing a roadmap involve:

➔ **Prioritizing services:** As already indicated in the name, this includes all the public services selected for priority implementation. These are the services - from the point of view of the target groups and from the administration, which can bring a particularly favourable cost-benefit-ratio when provided electronically. A further differentiation can be made to understand whether coordination is necessary across organizations or whether a decentralized

implementation is possible with the mutual exchange of experience.

➔ **Prioritized prerequisites:** In order to be able to implement the ‘prioritized services’, it is vital to coordinate the basic infrastructure (prioritized prerequisites), which generally concerns organizational, legal, standardization related and technical aspects. It basically describes and indicates what processes have to be harmonized and what kind of infrastructure has to be made available. The catalogue lists the basic prerequisites that must be developed with the highest priority. Some of the key activities that need to be carried out to provide a roadmap to the realization of e-government are depicted in Table 2.

Table 2: Key Activities for E-Government Realization

#	Activity	Description
1	Assessing E-government Readiness	Establish the state-of-readiness for e-government development and identify the potential stakeholders and their interests, and their willingness to provide input in order to develop a realistic strategy for e-government and to engage in the implementation of this strategy.
2	Formulating E-government Vision and Strategy	Engage the stakeholders in formulating the long-term vision for e-government and the goals, strategies and targets to realize this vision, based on the findings of the assessment and the lessons learned from other countries.
3	Constructing E-government Program	Set up a whole-of-government program by which the defined e-government strategy can be implemented across the government, thus engaging the stakeholders.

4	Building Human Capacity	Raising the capacity of the government workforce, including its leadership, management and technical skill workers to be able to lead, implement and maintain e-government operations, as well as the capacity of its citizens to be able to benefit from the e-government program.
5	Building Institutional Capacity	Strengthening the organizational capacity to be able to implement and benefit from the e-government Program constructed.
6	Building Research Capacity	Building local e-government research capacity, including the development and adaptation of methodologies, survey instruments, assessment tools and guidelines, as well as the capacity for strategic planning and program management and adapting international best practices to the local context.

4.8 Governing the E-Governance Transformation

After a review of the global practices, it was found that there is a strong empowered federal authority that drives e-government transformation. This exemplifies the structure of such an authority as having an ‘Advisory council’ and an ‘e-government Governance Council’. The ‘Advisory council’ provides valuable input and guidance, whereas the ‘Governance Council’ does the planning and resourcing. E-Government Authority (EGA) is the agency operating under the guidance of the ‘Governance Council’ to initiate and coordinate the implementation of various e-government programs.

Typically e-government authorities consist of ‘Working Committees’ on focus areas, ‘EGA Departments’ that carry out the EGA operations and ‘Partners’ who provide support services.

With the availability and the quality of services, assurances on Service Levels becomes a major requirement. A proper framework for service governance is required to be adopted. Several models exist for Service and IT Governance Frameworks. COBIT 5, ITIL provide an excellent guide. Based on standards, a Federal Service and an IT Governance Framework is proposed as outlined below. The Framework objects are further broken down into several sub-components with their own guiding principles and policies. Central to the service framework is Digital Identity Management. Service Beneficiaries and Service Providers interact with a high level of assurance in a secure transactional environment.

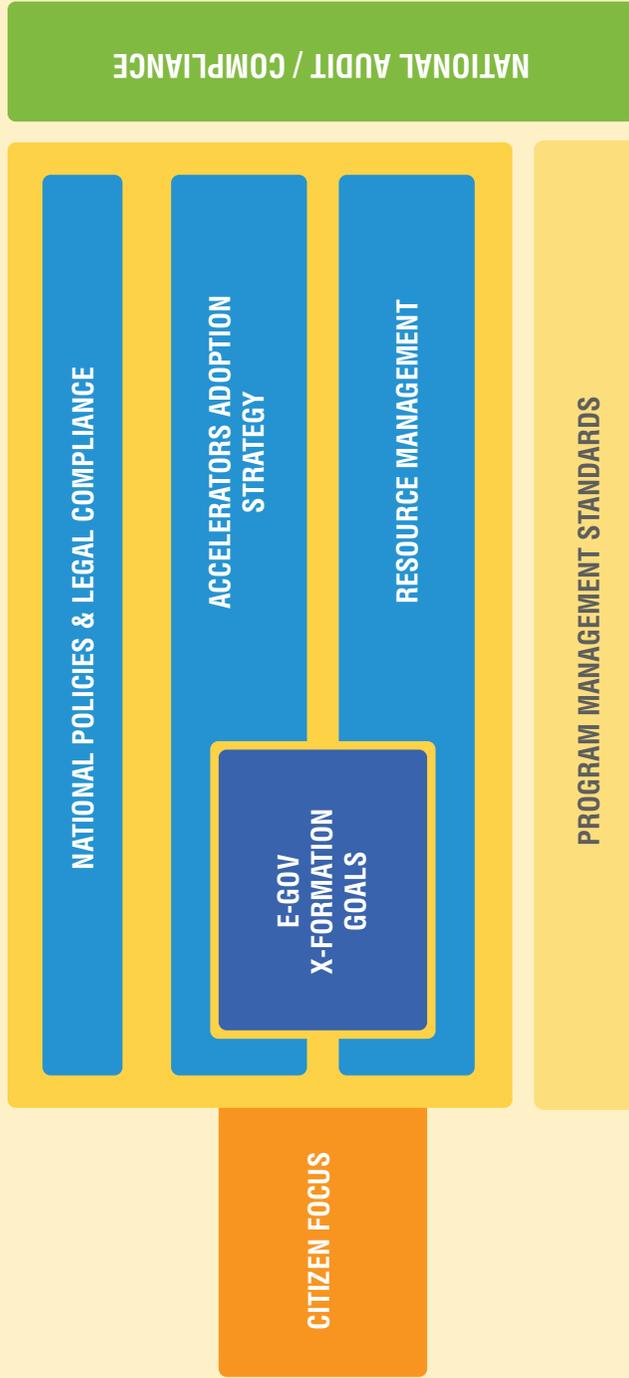


Figure 15. E-Government Transformation Management Governance Framework

4.8.1 Service Governance Framework

At the national level, a government agency vested with the responsibilities and the required executive authority would manage the government services. This authority would be the apex body in the country to regulate the services, and service levels as well as serve as an arbitration body for all services rendered by various government departments.

A central governance Committee would oversee the functioning of the Authority and be responsible for the services and service delivery to the citizens. This committee would be subjected to the Federal Government and Local Government Policies, in general, and would be backed by the country’s legal system, which would endow it with the pertinent legal authority.

Two other policies that would define the functioning of this Services Governance Committee would be the National IT Policy and the National Telecom Policy. These are the fundamental policies that would guide the delivery of the services across the multiple e-channels and process the automation which would lead to efficiency in service deliveries and optimization in service delivery processes. This would also lead to the standardization of the quality of services across the country.

Guided by these national level policies, the Service Governance Committee would have three major domains of functions:

1. Governance of Services.

2. Governance of Usage of Services.
3. Governance of the IT Systems.
(supporting the services and the service delivery).

4.8.1.1 Governance of Services

This would oversee the overall Services definition, the management of the service catalogue with defining the required service for different types of services and different service channels. This would provide the basis for defining the quality of services.

4.8.1.2 Governance of Usage of Services

This would deal with the beneficiaries' management and the actual delivery of the services. This would oversee the availability of the services and qualify the service beneficiaries and regulate the service delivery channels. 'How', 'When', 'Where', 'Why' and 'Who' are the components of the usage of the services, while governance of services would deal with the 'what'.

4.8.1.3 Governance of IT Systems

Information technology plays a major role in the service delivery and the service processes itself is an undeniable fact. IT Governance would deal with all the technical processes and the standardization of the technical infrastructure and the processes required to facilitate the service delivery.

From the governance, we look at the next level of the Service Framework components, which could be grouped as Implementation Objects of the Framework. This is guided by a clear Service Practice Statement and a well-defined Service Strategy. An SPS would be an unambiguous statement that would provide the vision as well as the set of practices that would establish the foundation for the service delivery and a commitment on the quality that would be provided.

As the government services organization would be a central authority, it would deal with National Infrastructure Development that would enable the services and the service delivery. This would not just include the logical infrastructure, but also the physical infrastructure. Thus, the development of the IT infrastructure/ computing systems, service centres, and service channels would be handled in great detail here.

On the other end of the development spectrum is the human capital development. Services development and delivery is not just the function of faceless machines, but is really made up of human interfaces. While humans are the consumers /beneficiaries of the services, is it possible these service deliveries would be driven by machines? Not so! They would essentially be driven by humans. The Human Capital Development would contribute greatly to the service organization, which could not exist without the human touch.

The four other components that form the implementation objects of the Services Framework are the Service Catalogue with all the services, service owners, service responsibilities,

service beneficiaries, the channels and service availability. Service channels would handle the different devices, locations and the means of the service delivery. It is critical to manage the last mile of delivery, which more often than not, defines end-customer satisfaction. The management of the service processes and the associated metrics for the performance provide the closed loop for the control.

At the base of the framework are the actual IT Infrastructure and the necessary technical devices that cover the backbone connectivity, the computing infrastructure, the security infrastructure and the integration of the technical and business processes delivering the quality services.

The central key component in the National Services Framework is the identity management and, more specifically, Digital Identity Management. This is the e-profile of a consumer/service seeker/beneficiary/provider along with their unique identity and the related credentials that establish, not just their identity, but also trust between the different stakeholders. This is the key factor to seek, deliver and benefit from the services across multiple channels of delivery in a seamless and ubiquitous manner. This lays the foundation for 24-hour service availability and the necessary assurance of a high quality secure service delivery.

4.9 Embracing Mobile Technologies in Transformation

Various governments have been utilizing short messaging services (SMS) for years to deliver timely and individualized information to mobile citizens. Modern smart phones are now equipped with desktop-class mobile web browsers that allow them to access a range of websites.

Mobile specific web pages need to be designed (both for smart phone and tablet sized screens) that offer a more limited selection of content targeted at mobile citizens. For example, the full PC version of the e-government portal may offer hundreds of options to the full range of information and services appropriate for PC consumption. Whereas, the mobile site can offer links to various information such as bus schedules, local weather, direct emergency contacts, and current polls, with links formatted as finger-sized icons rather than text, making the webpage resemble a mobile application (Campbell and Im 2012). Moreover, the web page can take advantage of advanced protocols to allow a user-initiated determination of the location of the device in order to provide location-based information about the nearest government offices, hospitals, rail stations, and other amenities.

Another example of mobile government development is Seoul's city-wide embedded bus schedule. Approximately, 7,600 buses serve over 5 million passengers every day in the city, with busses arriving on average every three minutes at city stops. Most major stops where multiple buses arrive are equipped with an LED display panel listing arrival times.

Since 2011, the city government has outfitted all of its over 6,300 stops with a small quick response barcode (QR code) that citizens may scan using their camera and some special software on their mobile phone. Upon scanning the QR code, citizens are taken to a special website formatted for mobile devices that displays routes and information about approaching buses in real time (Campbell and Im 2012). Global Positioning System (GPS) equipment on each bus relays its distance from the given stop thus giving passengers an accurate waiting time estimate that updates live as the next bus approaches. Soon after the embedded bus schedule was implemented, online inquiries about bus information increased over 125% from the previous year, with citizens polling the government data base an average of 200,000 times per day.

Several interesting ways are evolving in which a developmental model of mobile government would differ from that of the existing e-government models. This mobile government development model would better capture the new dimensions of government so would significantly extend existing models by augmenting and enhancing the existing services and would allow for easier access to existent information.

As mobile devices are designed primarily as communication devices, the early stages of m-government include various features and functions less common or impossible under the e-government paradigm, such as the ability to contact government offices directly from the phone, or to receive automated text messages about news or emergency information. As m-government advances, more advanced functionality is added including the possibility of E-voting

and online poll participation, and due to the dispersed nature of mobile technology, higher usage numbers are expected than the similar functionality that was available only from traditional PCs.

The communication model underlying this early stage of m-government is captured by the familiar G2C and G2B models, as well as by a C2G (citizen to government) model in its advanced phase. The next stage of mobile government development, however, represents a significant departure from the existing models of e-government.

We define embedded m-government as a mobile government strategy that makes location and time sensitive information available to citizens through environmentally situated electronic technologies such as QR codes, radiofrequency identification (RFID), or location-based technologies like GPS driven virtual environment overlays. This stage also departs from the familiar communication models, as it is no longer government information that is consumed in the strict sense, but rather information about the overall physical environment.

As such, under an embedded m-government framework, an environment to citizen, or E2C, communication model more accurately captures the information transaction that takes place. The most advanced stage of mobile government development we call 'coordinative', as it makes use of handheld devices to order and synchronize the behaviour of individual citizens with groups of other citizens within the mobile field. Thus, communication under this model can be characterized as 'aggregate to citizen' or A2C.

While we continue to use the phrase ‘mobile government’ to refer to the emergent phase, the term ‘m-governance’ is now used to refer collectively to stages two and three, in order to emphasize the discontinuous character of mobile technology. The m-governance paradigm removes many of the assumptions of the previous forms of e-government, which themselves are products of a pre-mobile government and citizenry. The replacement of ‘government’ with the less defined term ‘governance’ reflects the fundamental ambiguity between government and the governed that emerges in an advanced mobile framework.

4.10 Key Success Factors

Although e-government takes effort, there are some proven strategies that can help. The following critical success factors are crucial when planning, developing, and implementing new information technology initiatives in government.

4.10.1 Information and Data Strategies

Dealing with information, and data challenges require an overall plan for managing data and information products. A quality and compliance assurance program is an effective strategy for dealing with these challenges. Developing the appropriate data structures and definitions is critical to the success of IT initiatives, in particular for inter-organizational initiatives. The challenge in this area stems not only from gaining agreement that these are necessary, but also from engaging the necessary partners in the development and the

adoption of common structures and standards (Gil-García and Pardo 2005). Managers have attempted to minimize data-related problems by sharing standards, definitions and meta-data, with their potential partners. Getting continual feedback from users is also an important strategy to maintain data quality. Overall, having good quality and homogenous information seems to also be an important success factor.

4.10.2 Information Technology Strategies

Two technology-related factors that can promote the success of information systems are system usefulness and ease of use. Due to the relative complexity and newness of some technologies, a strategy for responding to information technology-related challenges is to organize presentations about the technologies, which can build awareness as well as to focus early efforts on developing system and process prototypes. Strong technical skills and expertise in the hands of the project leader and the team members is critical. It is also important to take into consideration the potential shortages of qualified technical staff. An incremental approach may help in dealing with this problem.

4.10.3 Organizational and Managerial Strategies

Establishing clear and realistic goals is an important factor for the success of IT initiatives. Identifying the relevant stakeholders and getting them involved in the project development process, especially end-users, has also been found to be an effective strategy in overcoming organizational and managerial challenges. Strategic planning techniques can be seen as an umbrella for more specific strategies such as clear milestones and measurable deliverables; good communication channels; and previous business process improvement. It is also imperative to maintain the current skills and training needs of both the developers and the end-users. Successful projects need a finely tuned and balanced combination of technical, managerial, and political skills and expertise among their members. Finally, financial resources are not always the most important factor, but are necessary. Often, managers need to develop innovative financial schemes and partnerships to get e-government initiatives off the ground.

4.10.4 Legal and Regulatory Strategies

Restrictive laws and regulations developed prior to or in ignorance of the technologies relevant to e-government can jeopardize the success of projects. One strategy for responding to these challenges is to invest in changes to the regulatory environment that allow for or enable the adoption of emerging technologies. Digital signature technologies, for example, required statutory

changes in most jurisdictions before they could be adopted for use. The development of appropriate government-wide IT policies and standards can also provide an adequate framework for e-government initiatives to be successful. In this regard, state governments are developing IT policies and standards and making them available through their official Web sites.

4.10.5 Institutional and Environmental Strategies

Individual leaders or managers cannot change institutionalized rules or practices. However, if a coalition is large and varied enough to capture the attention of legislators or other policymakers, some formal institutions can be changed. There are at least two strategies to deal with institutional and environmental factors: getting executive and legislative support; and using outsourcing strategically.

4.11 Conclusion

The e-government strategy is underpinned by basic concepts, base components and open standards, which serve as guidelines for the implementation of the electronic services and the creation of the underlying infrastructure. The development and implementation of electronic public services is one of the priorities of governments across the globe. Citizen-centric governments envisage that every citizen in every community should have access to all forms of e-government at the federal, provincial and local levels. Secure

communication and the confidential handling of transactions of personal data thus have top priority. e-government will do more than just improve services, save costs, make work processes more efficient, and enable independent work. It will also make communication between citizens, businesses and the government more transparent, and open up new possibilities for the way in which information is presented and accessed. One of the most important promises of a transformed e-government is that it offers more opportunities for participating and having a voice in community matters.

5

ENTERPRISE LEVEL THE TRANSFORMATION OF INDIVIDUAL AGENCIES AND DEPARTMENTS

5. ENTERPRISE LEVEL THE TRANSFORMATION OF INDIVIDUAL AGEN- CIES AND DEPART- MENTS

This chapter will go into more detail regarding the different facets of bringing the e-transformation to the individual agency and department levels. It also outlines the broad challenges and projected roadmap in this entire exercise. It also defines and lists the measurement methodology and metrics for the levels of success of this envisaged transformation. As well, it maps the results achieved and the progress made towards the Transformational Vision.

Governments function through autonomous bodies such as agencies or departments. Each department services specific sectors like banking, healthcare, education, transport, telecommunication etc. Traditionally, these departments worked as islands. With the advent of e-government, more value can be seen through the integration of these silos, which thus creates an impression of a single government or citizen-centric government.

5.1 Issues and Challenges in Bringing Transformation to the Agencies

The indicators of e-government at the country level are widely accepted and commonly used as opposed to at the agency or regional levels. Agencies share some of their e-government requirements with those at the national level, like interoperability, security, and user friendliness. Besides these, agencies also have specific requirements that are either unique to their context, or because of their characteristics, demand more attention. These include cost and resource considerations, enhanced accessibility and greater scalability due to the larger number of citizens and businesses served. (Nabafu and Maiga 2012).

The prerequisites for an agency or even a local e-government differ in comparison with the national e-government by way of having fewer and limited resources, as well as the necessitating theories and models to deal with these aspects. The factors for the successful implementation of local e-government projects are:

- The need to adapt and fit the guiding principles and strategy for local e-government to those communities being served.
- Top leadership and political support.
- The financial shortages requiring that priorities be set for normative, strategic and operational control.

- A seamless integration of administrative processes at the agency/local, central or federal level.
- Integrating competence and greater qualifications into the comprehensive strategy of local e-government.
- Staff motivation and training.
- Compliance with the legal provisions.

5.2 Importance of an Agency Enterprise Architecture Strategy Aligned with Federal Enterprise Architecture

Enterprise architecture can be viewed as a link between an organization's strategic plan and the program and supporting system implementation investments that it intends to pursue to systematically achieve its strategic goals and outcomes. As such, the architecture is basically a blueprint, defined largely by interrelated models, that describe (in both business and technology terms) an entity's 'as is' or current environment, its 'to be' or future environment, and its investment plan for transitioning from the current to the future environment. The use of such a blueprint is a recognized hallmark of the organizations that effectively leverage technology in the transformation and modernization of business operations and supporting systems. The Federal/National Enterprise Architecture is intended to provide a government wide framework

to guide and constrain federal agencies' enterprise architectures and information technology (IT) investments.

The Agency level of architecture provides an overview of the entire department/agency as well as consistent, decomposable views of all sub-agencies/bureaus, business units, programs, systems, networks, and mission or support services. The depth of documentation in any particular area of an agency's architecture is determined by the need to support planning and decision-making, prioritized in the context of the agency's strategic goals and business operating plans. A drill-down is accomplished through the completion of segment, system, and application-level architectures. (Office of Management and Budget 2012).

Enterprise Architecture (EA) provides a blue print for the ICT transformation of enterprises. The realization of the EA comprises many stages. The following diagram illustrates stages for realizing the Enterprise Architecture initiative.

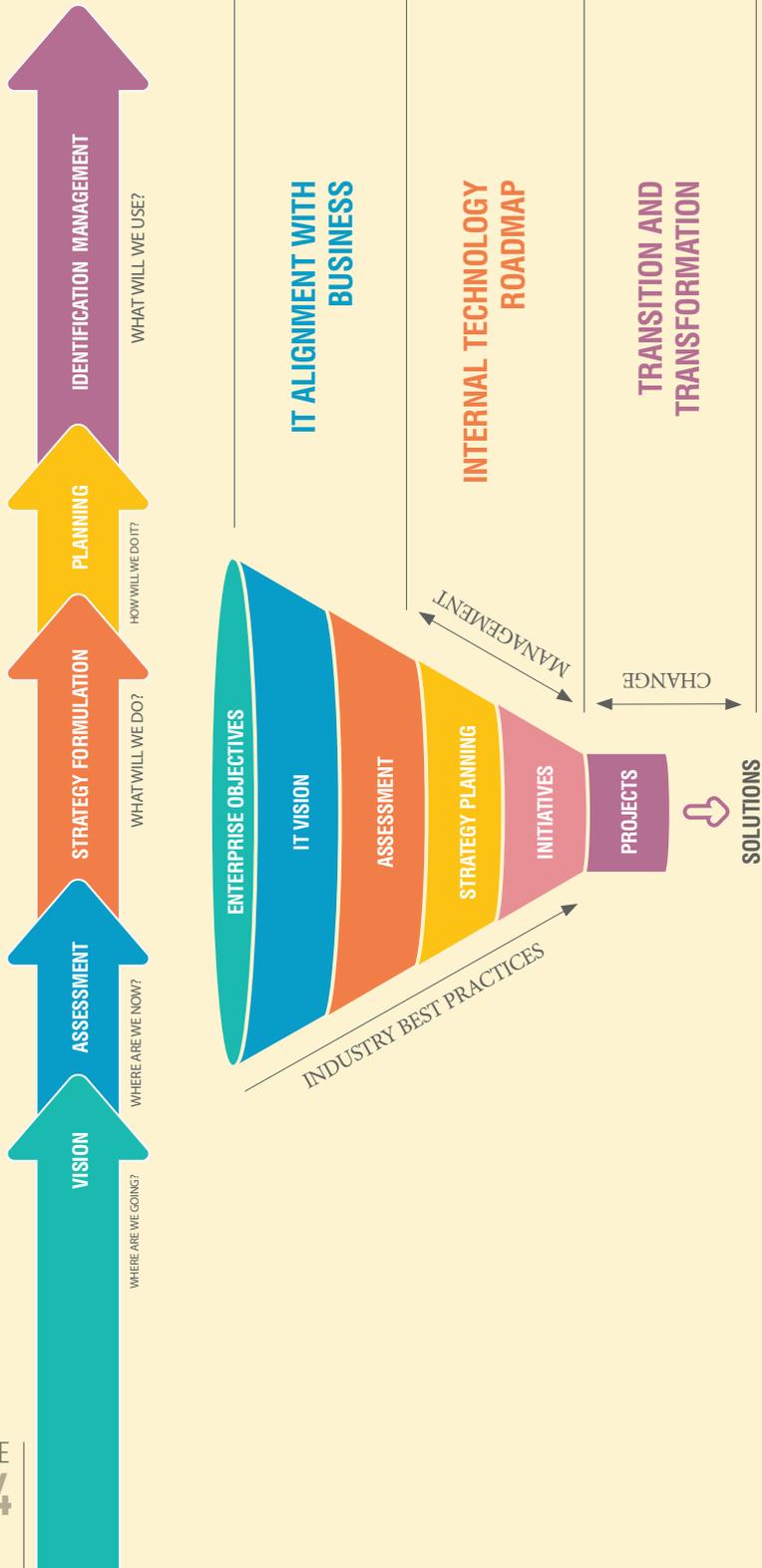


Figure 16: Enterprise Architecture Strategy

The strategy starts with the definition of the Enterprise Architecture’s vision and objectives. This is followed by the assessment of the current state or ‘as is analysis’, which brings out the strengths and weaknesses in the existing system to meet the organizational goals. Subsequently, strategies are formulated to overcome the gaps identified during assessment. Based on these strategies, the appropriate solutions need to be identified, then the proper planning is required in order to draw a roadmap for the implementation. One major aspect of the successful implementation of any EA strategy is to determine whether every project is aligned to the business objectives.

5.3 Role of Interoperability Standards and Frameworks

During the last few years, e-government interoperability has become a vivid and fascinating research and development issue in order to facilitate the seamless exchange of information across governmental departments. To advance in this direction, several approaches have been proposed through the adoption of frameworks or through architectures to each other and to the environment, as well as to the principles that guide its design and activity.

With regards to the frameworks, the Electronic Government Interoperability Framework or e-GIF facilitates this. The e-GIFs are defined as a set of standards and guidelines that set out a common language to ensure the coherent flow of information across systems. In many countries, governments have developed their own

e-GIFs such as the UK e-GIF, New Zealand e-GIF, the European Interoperability Framework (EIF) and the Australian Government Technical Interoperability Framework (AGTIF).

In addition to the achievement of the interoperability of e-GIFs, the architectures have an important role to play in ensuring the success of e-government interoperability. The relevant architecture to electronic government interoperability is Enterprise Architecture (EA), which is specifically the National Enterprise Architecture (NEA). The EA stresses the planning and management of all IS assets and their architecture together with organizational structures and processes.

However, implementing interoperability in government requires more than just having a common technical standard to create a technical integration between two applications. The challenges and obstacles that governments face in implementing electronic government interoperability include:

- 1) Bureaucratic challenges due to the nature of bureaucracy and the lack of accountability of different agencies.
- 2) Ensuring compliance or the enforcement of the adopted standards.
- 3) Capacity development.
- 4) Using the right metrics to measure the success of the e-GIF. In fact, the bigger and more complex the bureaucracy, the more difficult it is to implement it.

Many governmental departments still have entrenched cultures, which avoid openness and cooperation with others. This makes the implementation in government interoperability become more difficult. Moreover, in complying with e-GIFs, there is no guarantee that other agencies will truly follow. Therefore, merely following the suggested open standards, policies and context guideline as well as the EA approach is inadequate. The successful implementation of e-government Interoperability needs a more practical approach.

There are many obstacles and barriers to e-government interoperability, which originate from technical, semantic and human issues. The technical obstacles refer to the great variety of legacy systems, which are systems already installed and running within involved agencies. By replacing these systems in order to achieve interoperability is not feasible. The semantic barrier is concerned with the difference between data/information standards used within organizational services. Understanding the semantics of each service is also an important issue. Another important obstacle to the spread of interoperable solutions in e-government is that of the adoption of any new systems by officers. The interoperability barriers also include cultural differences between governmental departments, issues of trust, timing, collaboration between agencies, unsatisfactory workflows, convincing stakeholders of the importance of the system, legal issues as well as the importance of political support and funding.

The benefits of being able to achieve e-government interoperability are numerous and significant. From the standpoint of public services, we argue that addressing interoperability challenges will

not only improve the efficiency of service delivery, but also access to the services, the coordination among existing services (resulting in further efficiency gains), and technology management and maintenance. In addition, the administration can avoid potential future costs such as inflexibility due to vendor lock-in and the high price of new development by leveraging existing systems in new ways.

From the standpoint of policy makers, e-government interoperability will improve data gathering and parsing techniques, which would also result in more efficient decision making as it would be based on more accurate information. Improved interoperability will also enhance transparency and accountability, thus resulting in better overall governance. (Novakouski and Lewis 2012).

The context for every e-government project is different as different services require different technologies, different semantics, and different processes, and are also influenced by different factors. The combination of the desired services and the context in which the provider will deliver them drives the interoperability requirements. While frameworks and models can certainly help set expectations and can help focus on problems, assigning maturity levels often results in an implication that 'higher is better'. Instead, it can be argued that the correct approach is to find the level of interoperability that best delivers the specific public service or services being developed. Especially, in e-government, interoperability is not necessarily machine to machine. There are many cases in which the solution is human to machine or even human to human. The following sections provide examples and guidance that can address some of the

challenges for systems' interoperability in the e-government context.

To enable information exchange at any level, governments must select the most compatible technology solutions (Novakouski and Lewis 2012). This can be as simple as standardizing a form or restricting communication to phone calls or as complex as selecting web service security standards. Regardless of the selected technology solution, service designers must consider a number of issues to ensure that the technology solution is appropriate. This effort should begin by examining how e-government stakeholders have historically attempted to solve the problem and then identifying the issues relevant to their context.

To support semantic interoperability in a technological context, public service providers have to agree on several characteristics of the data to be exchanged, including data attributes such as:

- Units (e.g., metric versus imperial units).
- Validity (e.g., retirement-related information is valid only if the age of the person is above 65).
- Time period (e.g., a policy may not apply if an event occurred during a certain period of time).

Achieving semantic interoperability is a difficult problem that is largely left unsolved within the e-government context. Stakeholders typically achieve semantic interoperability through a direct negotiation until they reach a consensus. One common approach

to building this consensus is to construct an ontology or a set of ontologies, which are basically data models that define the data items to be exchanged - including the exact meaning and structure assigned to them as well as the relationships between the data items.

To enable organizational interoperability in the e-government context, public service providers have to agree on, not only what information is to be exchanged, when it is exchanged, and how it is exchanged, but also what to do with it when it is exchanged. Stakeholders typically achieve organizational interoperability in a manner similar to that of semantic interoperability, by negotiating directly in order to come to a consensus on the processes to be used. Addressing organizational interoperability is also similar to addressing semantic interoperability: The process is primarily manual, and a few tools are available to automate the process. The processes evolve in ways similar to data models and technological standards so thus incur the same maintenance costs. Agreement by communities of interest on the processes to be used can also be hard to reach for the same reasons and also because different organizations tend to use different business processes to create competitive advantages. Different organizations also have different (and sometimes directly conflicting) goals, so there may be scenarios in which technical and semantic interoperability exists between two government entities, but because of competing goals, the organizations cannot agree to work together.

Technology interoperability is in the context of two or more technology components interacting together. The standard reference

models for a technology stack and application platform should guide technology interoperability. The following diagram illustrates the technology stack reference model for e-identity integrated e-governance.

This technology reference model consists of four layers:

- External Entity Interface
- Infrastructure
- Platform
- Solutions

The infrastructure layer is the core of the stack and consists of all the hardware, system software, networking and security components. The Platform is the set of common services and components that is implemented to support applications. The Platform removes redundant components from the applications in such a way as to make the application development easier and light weight. A standardised infrastructure interface will help the platform insulate itself from the changes in the infrastructure. The Platform exposes the standard set of APIs that can be used from the applications to perform various tasks. External Entities can be the services provided by the identity provider, PKI services, or Payment Gateway etc. which need to be integrated with the enterprise systems. The Platform also provides integration with the external entities in a standard manner and makes the external services seamlessly available inside applications.

As we can see, the technology reference model is complicated and

consists of numerous components and interfaces. An empowered standardization committee should oversee the defining of it and its compliance to the technical interoperability standards.

As we have seen, system interoperability is contextual. A corollary to this statement is that interoperability is not a characteristic of a single system, but rather a characteristic of the relationship between two or more systems in a particular context. The context in which systems have to interoperate shapes the requirements that each individual system has to satisfy in order for it to interoperate with those other systems. Thus, developers need to plan system components around both technical and non-technical aspects of interoperability.

A development team can analyse interoperability in any context along technical, semantic, and organizational dimensions, but the diversity and complexity of the legal, political, and socio-cultural dimensions of the e-government context make interoperability challenging for all e-government systems.

5.4 Metrics and Measurement for Agency Level Transformation

There is a growing recognition worldwide that effective public sector governance requires the use of ICT to achieve more efficiency in the functioning of government and to, thereby, improve the delivery of government services for both organizations and individuals. In order to measure and compare the incidence of e-government, a set of feasible, relevant and comparable, indicators

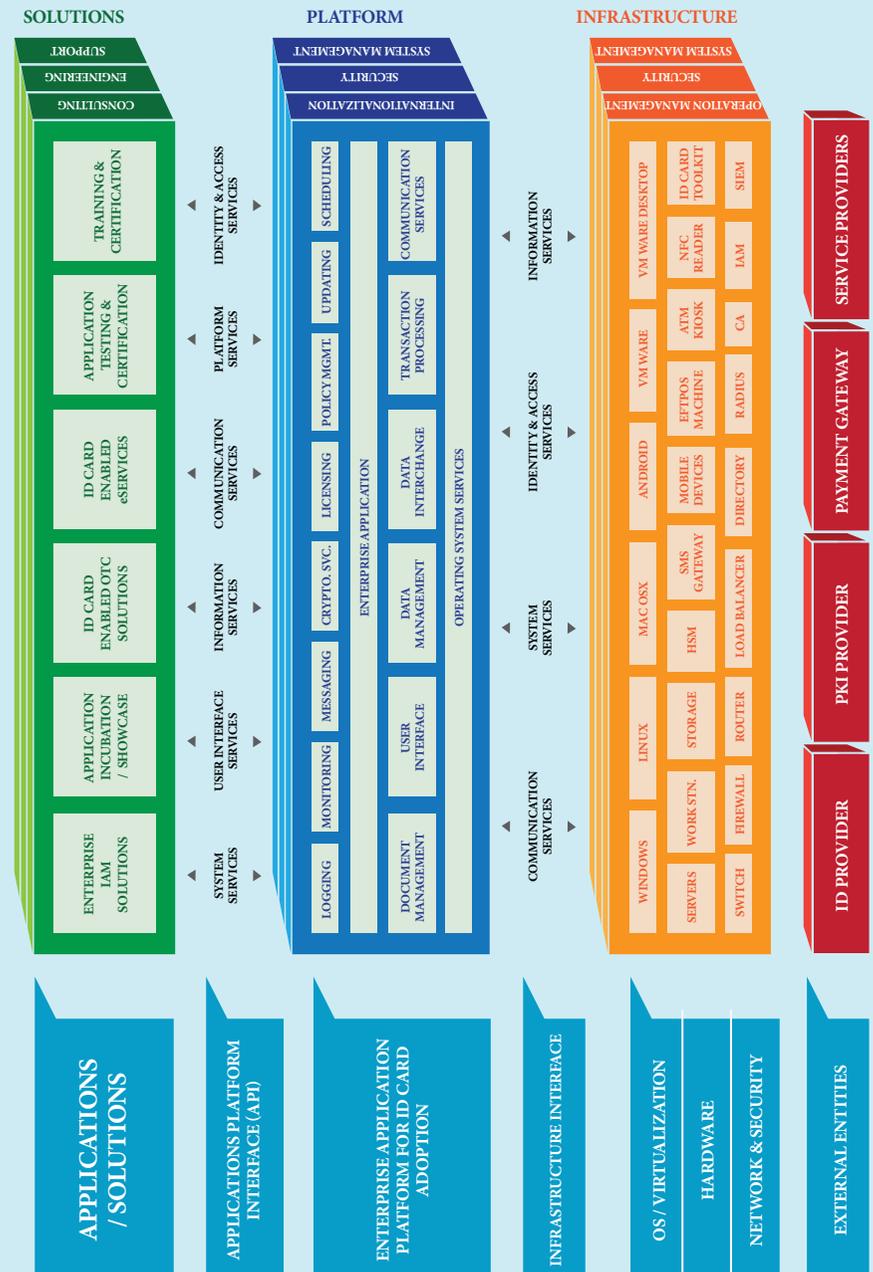


Figure 17: Technology Stack for System Interoperability

is required. Such indicators are useful input to the formulation of policies and strategies for effective government (Partnership on Measuring ICT for Development 2011).

In order to assess e-government, individual indicators and composite indices have been developed by international organizations, academic establishments and individual countries. The scope of interest in this area includes single countries, regions and global measurement. Some studies assess the use of ICT alone; while others measure customer services through the services offered via government websites, which can range from simple services to more sophisticated issues of privacy and electronic voting.

E-government indicators, as a policy tool, reflect both the status and trends, which can be used as a guide for policy-making and lead toward a more efficient administration, improved services and more equal participation for citizens. As such, they are anchored to technological platforms, which provide computing, storage, communication and access services.

While an increasing number of governmental units are incorporating or expanding the use of Information and Communication Technologies (ICT) into many of their activities, little is known about whether citizens are getting the information and services needed or about the state-of-the-practice of e-government at the local community level across the nation.

Also, effective and agreed-upon measures to evaluate the quality of e-government are lacking. Most existing measures are quantitative

(e.g., number of websites, decrease in response time to questions, etc.), but few include qualitative measures related to policy and ethics, such as the level of satisfaction by citizens with the quality of service, or whether privacy policies are included on websites and whether local government officials are aware of the need for privacy protection, etc.

Although some efforts are being made to develop metrics, no systematic set of quantitative and qualitative measures has been yet developed for widespread use. In addition, many socio-cultural, economic, and political implications of the use of IT to provide government information and services (e.g., increased expectations of citizens for more and better services and concerns about the violation of citizens' privacy) have not been sufficiently addressed. Finally, many local government officials are being asked to take on e-government responsibilities with little or no education or training and no comprehensive educational programs exist that can provide the competencies needed for an effective e-government or can provide the necessary continuing education modules for individuals to gain the competencies needed and to update their knowledge and skills besides, many e-government services to date have been created by agencies based on the existing services and on their understanding of what is wanted and needed, rather than being designed from the citizen's needs and interests. As well, often little data is available about what local government officials and citizens really want and need. Metrics for the development and evaluation need to be tailored to the technical, personal, ethical, organizational, political, social, cultural and economic characteristics of a community and the government agencies that serve that community.

In addition, metrics must incorporate the stage of development that the e-government system has reached and the services offered in that community, recognizing that multiple delivery mechanisms are often needed. No 'one-size-fits-all' model or single set of metrics is necessarily appropriate for all e-government systems and services. Success metrics may well vary depending on the project. For example, the successful connection of information in databases from several different agencies at different levels of government might increase the potential for the violation of individuals' privacy.

Among measures to be included in the metrics are:

- 1) Innovation and use of IT to deliver government information and services.
- 2) Efficiency.
- 3) Return on investment.
- 4) Ease of use.
- 5) Focus on citizens' needs.
- 6) Ease of navigation across levels of government.
- 7) Protection of privacy and inclusion of privacy policies.
- 8) Security and ease of auditing.
- 9) Inclusion of qualitative and quantitative measures.
- 10) Evidence of public and private partnerships.
- 11) Effective evaluation mechanisms.

While performance measures have been widely used for assessing traditional forms of government service delivery, agencies have been generally slower in developing their own measures to assess the delivery of services through the Internet. (Nicoll, Robinson and O'Hanlon 2005) Many agencies use a range of methods to

collect performance data and some of them have determined some performance indicators for their online services.

However, it is rare that agency collected information enabled a comparison of the efficiency of online service delivery against other service delivery channels. Overall, the general measurement practices followed today are inadequate to assess whether the delivery of government services and programs through the Internet is efficient and effective.

The best practices for an effective performance measurement of e-government are:

- Project initiatives should be supported by a suitable cost-benefit analysis.
- Agencies periodically evaluate their websites and Internet services to confirm that they meet the needs of both the agency and the clients.
- Agencies integrate the measurement of their website's performance with the overall measurement of service delivery.
- Develop indicators, which include data on costs, for the performance of their online service delivery.
- Compare these with similar indicators for other service delivery channels.

The development of a business case should be the agency's first step in considering the delivery options for any service, as that underpins the decision and any cost-benefit analysis and can be the focus for later evaluations and audits. Once the service has been implemented, the agencies can revisit their business case to consider whether the service delivered as intended, and whether it did so efficiently and effectively. This applies whether the service is provided through the Internet or through other service delivery channels.

5.5 Supervision and Compliance

A central coordination is the basic feature of the strategies for e-government that are promoted by the Organization for Economic Cooperation and Development (OECD). In general, central e-government coordination involves a formal organizational unit located within the Public Administration or linked to a broader Information Society.

Several approaches have been applied that provide central coordination. These include establishing a government agency dedicated to e-government coordination and forming a committee of agency heads or Chief Information Officers. The involvement of non-government representatives from industry, academia and other organizations has also proved effective.

e-government projects generally require stringent internal supervisory measures to ensure that they achieve the defined goals and objectives. As well, government auditors evaluate the system and

process controls to gauge their adequacy and to establish the audit scope for cost and benefit analysis. The following diagram illustrates the steps required to monitor the performance of an e-government program.



Figure 18: Steps of E-Government Performance Monitoring

The highest degree of supervision comes from individuals who are competent in - and independent of the process being reviewed. However, other internal elements are significant. These include:

- Peer reviews
- Management evaluations
- Periodic metrics
- Exception report analyses and
- Routine surveillance.

Regardless of the methods used, the evaluation processes must include some mechanisms for bringing non-compliance findings to the attention of the e-government authority, as well as the resolution of the problem issues. The following are some of the important aspects that ensure effective supervision and compliance:

- Establish the indicators, metrics and measures, whereby, project overseers can identify the expectations of the e-government stakeholders.
- Develop metrics, identify exception reports, and document any departmental or peer reviews that are routinely performed to verify compliance. Consider a complete evaluation of each business system by competent independent evaluators every three years.
- Develop and maintain procedures for reporting, resolving, and following-up on non-compliance findings.

The monitoring and evaluation of government projects are increasingly recognized as vital management functions.

Policy-makers and project managers can use benchmarks, key performance indicators (KPI), user satisfaction surveys and other monitoring and evaluation tools to track the performance of e-government projects and to determine whether mid-course adjustments are needed.

Monitoring and evaluation should occur throughout the

implementation of a project, to measure progress, support mid-course corrections and to guide resource allocation decisions. This may occur at various levels of an e-government project. At the project level, the project team must continuously monitor the project's compliance to the set of identified standards and policies related to the project. Also, a monitoring and evaluation team from a central government e-government coordination agency would need to monitor the project against any selected set of standards and policies identified from the project initiation stage.

5.6 Conclusion

Agencies thus have a vital role to play in e-government. It is important to have national level strategies, governance and enterprise architecture to streamline the e-government initiative at the national level. However, it is the agencies and the local governments that are responsible for delivering the services to citizens. Agencies, therefore, need to align themselves with the national vision and the appropriate strategies for e-government transformation. This needs to be strengthened with the adequate metrics that can measure the performance of e-government at the agency level. Finally, stringent monitoring and evaluation is required to assess their compliance with the national e-government strategy and roadmap.

6

NATIONAL IDENTITY MANAGEMENT SYSTEM BUILDING TRUST IN E-GOVERNMENT

6. NATIONAL IDENTITY MANAGEMENT SYSTEM BUILDING TRUST IN E-GOVERNMENT

The trust of a government's citizens, which is essential to the adoption of an e-government, has two components: trust in government as an institution and trust in technology (Colesca 2009). Unlike the traditional physical transactions where citizens interact face to face with the officials of government institutions, today's electronic transactions are virtual, and performed interpersonally between strangers and abstract systems, so the familiar ways of establishing trust are markedly absent.

Citizen concerns about inadequate security and built in privacy safeguards in the electronic networks can lead to a distrust in the applications of e-government. This distrust can be due to the concerns about unwarranted access to sensitive personal information or vulnerability, to online fraud or identity theft. Such concerns can be a major impediment to e-government services. Trust, security and transparency are the major issues which could become barriers to the adoption of e-government. Various studies have identified some major factors that affect citizens' trust in e-government. These are:

- Privacy concerns
- Perceived organizational trustworthiness
- Trust in technology
- Citizens' higher perception of quality and usefulness of e-government.

Studies suggest that there are 6 possible benefits of e-government that could lead to an increased trust and confidence in a government:

1. **Responsiveness:** Improved communication and interaction with citizens.
2. **Accessibility:** Round the clock, seven days a week.
3. **Transparency:** Making publicly available data, policies, laws, meeting schedules, minutes, and contact information.
4. **Responsibility:** As demonstrated by privacy and security statements and policies for handling personal information submitted online along with government data that is posted online.
5. **Efficiency and effectiveness:** Through the use of the latest technology to automate processes, improved service delivery, produce budget savings, and save time.
6. **Participation:** Takes into account, citizens' input and suggestions.

Signalled out government waste and inefficiency as reasons to an underlying current lack of trust in government. This, is in line with the philosophy, a government that works better and costs less will increase citizen confidence in government. E-government thus has the potential to reduce the cost of service delivery; although, the

upfront costs of development may mean that the cost savings are not immediate.

The generally positive perceptions indicate that e-government is worth pursuing as a means of enhancing the effectiveness of government agencies and their relationships with citizens. In this chapter, we will delve into detail regarding the aspects of security, privacy, effectiveness and the overall technology aspects that affect the trust of citizens in e-government. Institutional trustworthiness and transparency are factors outside the scope of this book.

6.1 Last Mile Challenges in E- Service Delivery

As mentioned earlier, in the context of e-government, transactions happen between abstract entities or objects. For the e-government system, a citizen is an abstract entity and for the citizen, e-government is another abstract entity and a black box. Citizens consume the public services over e-government channels through virtual transactions. The transition from traditional government

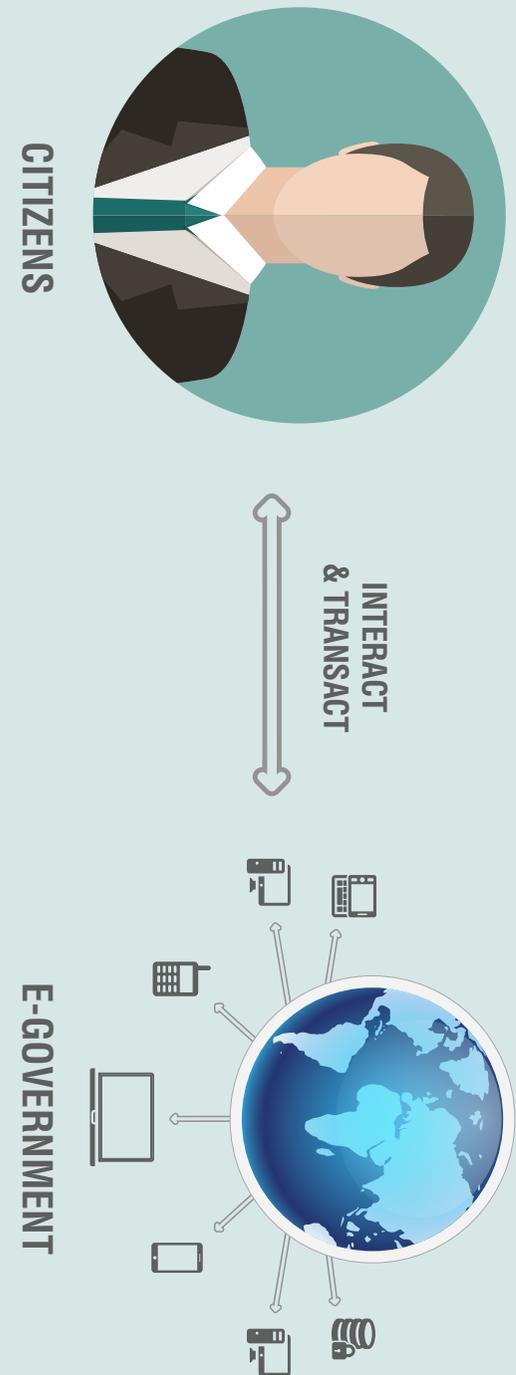


Figure 19: E-Government Citizen Interaction

to e-government pushes citizens into an unfamiliar and strange territory. This strangeness or unfamiliarity causes the e-government to start out initially with a low level of trust.

In this virtual environment, as mentioned before, where abstract entities of citizens and e-government systems are involved in virtual transactions, the traditional and familiar ways of establishing trust is absent. This scenario is similar to the advancement of banking systems and the entry of ATMs. Due to concerns about security, there was initial resistance and inhibitions among banking customers towards the use of these technologies such as with the use of the debit cards, credit cards, and ATM machines as well as with Internet banking.

Various stories published in the press regarding fraud exploiting vulnerabilities in these technologies only helped to magnify this fear. This fear can be primarily attributed to the lack of familiarity with the technology and also with shortcomings in the implementation of the technology by the banks. Over time, this inertia was overcome with citizens becoming increasingly familiar with the technology and the attractiveness of the benefits that came along with it.

Banks also adopted various best practices that were evolved from the lessons learned in order to tighten the systems and fix the vulnerabilities. This case underlines the previously mentioned aspects of trust which is a citizen's perception of quality and the usefulness of e-government as well as trust in the new technology due to an increasing familiarity with the e-government technologies.

In a virtual environment, being able to reliably identify and authenticate citizens is the primary challenge before being able to authorize them to avail themselves of any e-government services. Again, in the traditional manual methods, a visual inspection of identity documents helped officials establish the identity of citizens. The call for more automation, aimed at improving the efficiency of the government process requires automated, electronic methods of identification and authentication. Fortunately, the advancement in technology is coming to our aid with many reliable and secure options that can facilitate this automated identification and authentication of individuals.

The electronic means of identification and authentication does require individuals to carry a trusted identity document, which can be used electronically. When considering these technologically enabled identity documents, it is imperative to look at the new possibilities thrown open by these technologies. Perhaps, this new means of electronic identity documents can securely hold more information about the citizen's entitlements. Hence, all the initiatives should be looked at from a new perspective of innovation rather than from just automating the traditional manual processes.

6.2 Trust Enhancing Technologies

From the beginning of the ICT revolution, security has been one of the major challenges faced by its users. Confidentiality, integrity, authenticity and availability have been the main constituents of ICT security. Cryptographic techniques have helped ICTs achieve a high

level of security in each of these constituents. Some applications of cryptography are encryption, digital signature and the integrity of digital data.

One type of cryptography called ‘public key’ is of special interest in the context of e-commerce as well as e-government. This is because: using this cryptographic technique we can enable remote authentication of individuals electronically. RSA algorithm which is named after its three inventors Rivest, Shamir and Adleman is the most popular public key cryptography technique available today that can be used for encryption and digital signature. Many standards, processes and best practices evolved around this technique, collectively known as Public Key Infrastructure (PKI) which is the most prominent trust enhancing technology available today.

The term “electronic signature” is often used incorrectly. An electronic signature refers to a signature that is processed, stored or transmitted electronically. This includes, but is not limited to, electronically transmitted documents bearing handwritten signatures, such as a PDF document with a handwritten signature, and digital documents that have been encoded with an electronic signature (Castro 2011).

Digital signatures are an important subset of electronic signatures. Digital signatures use a technique known as asymmetric cryptography that requires two components: a private key for the sender to sign a document and a public key for the receiver to verify the signature. The keys are generated by a certificate authority who is a trusted third party such as a private company or the government. Certificate

authorities issue digital certificates that contain public keys, along with information about owners and the cryptographic protocols used. The certificate is signed by the issuing certificate authority and is valid only for a specified time period. The public key infrastructure defines a set of certificate authorities for digital signatures and the trust relationships between these certificate authorities. Digital signatures can provide three critical cryptographic functions.

First, it can be used for authentication. The receiver of a message that has been digitally signed can verify the signature to authenticate the identity of the signer of a message.

Second, digital signatures can provide integrity. Using a digital signature, the receiver of a message can verify that the message has not been modified.

Third, digital signatures can be used to provide non-repudiation—the property of being able to prove to a third party that the signature was provided by the signatory.

Digital signatures occur frequently in electronic transactions, not only between individuals, but also to securely pass information between electronic devices or applications.

Globally many regulations are enacted to promote e-commerce which gives legal validity to digital signatures. Hence digital signatures can form the foundation of attesting transactions in a virtual environment in the same way handwritten signatures are used traditionally. Now that we have found a reliable way to establish

authenticity of transactions remotely, one major challenge is left: how do we enable citizens to handle the private keys securely and conveniently?

In olden days, people carried paper documents to prove identity. Today, these identity documents are replaced by plastic cards which are more durable and convenient. All these documents whether paper or plastic carried printed data on the surface which enabled visual inspection.

The plastic identification document or card in its new avatar called smartcard incorporates a processor chip that can store and process information electronically. With this capability, you can consider the smartcard or chip card as a miniature computer. Adding more punch to this technology, smart cards come with on-board cryptographic processing capability which means the card can not only store sensitive data such as the private keys but also perform cryptographic operations such as digital signing. If we enable the smart card with individual private and public key pair, the cardholder can securely carry it around like a credit card and use it at designated usage points.

This solves the problem of trust as long as the cardholder is in possession of the card. What if the card is lost or stolen? How do we electronically verify if the individual who is carrying the card is the real owner of the card? Biometrics perhaps?

Biometric technologies enable the identification of individuals based on their physical characteristics such as fingerprint, iris etc. Also, today's technologies enable smart cards to hold the biometric

data of the cardholder. The biometrics of an individual who is presenting the card can be verified against the authentic biometric data of the cardholder stored in the card to prove the ownership of the card.

The self-containment of smart cards makes them resistant to attack and capable of securing PKI private keys of the owner and can perform the cryptographic operation on card without relying on potentially vulnerable external resources. It provides PIN protection to the critical card information and some of the cards even provide capability to match biometric templates on the card to authenticate the owner. Facility to generate the key pairs inside the card ensures that the private key is never copied anywhere outside the card. Smart card and PKI provide two factor authentications which can stand against most of the authentication attacks known. Hence, it is evident that PKI, smartcard and biometric technologies complement and fill the shortcomings of each other and when combined form the strong foundation of trust enhancing technologies.

6.3 A System for National Identity Assurance

The e-government revolution, started in the '90s, envisaged a change that has been incremental. With technology still evolving but with the lack of reference models, with high costs and risks, made this strategy look apt at that time. Most e-government initiatives during that period were aimed at creating ICT infrastructure and service delivery over the Internet. These initiatives were fragmented

and lacked a common strategy, which resulted in duplicate IT expenditures and wasted resources.

As a by-product of these fragmented initiatives, today, government agencies operate numerous systems that utilise personal identity information. A vast majority of these systems were owned and operated independently from one another. These facts contribute to several issues:

- Duplicative identity data is stored in multiple locations within and across the agencies.
- A lack of commonly used standards makes appropriate cross function collaboration difficult.
- Privacy protection policy and efforts vary across agencies.
- No single government-wide forum is responsible for unifying Identity Management (IdM) efforts across the government.

Digital identity cards issued to individuals are becoming used in an attempt to resolve these problems. Digital identity is a set of attributes that connect that identity to an individual. The management of this digital identity system involves technical systems, rules and procedures that define the ownership, utilization, and safeguarding of personal identity information. All personal identity attributes are not created equally. Some are useful for a broad range of applications, while others are only useful within the context of a specific

application and should not be shared outside that application. The identity information within both of these categories also has varying levels of sensitivity and should be managed accordingly.

A federated approach to digital identity management leverages broad-use identity attributes to maximize accuracy, availability, privacy protection, and management of this data. Common technical standards and policies are required to ensure appropriate use and control.

Globally, government ICT think tanks are increasingly becoming aware of the problems arising from managing identity silos and the overhead caused by such a redundant infrastructure. Also, there is a growing consensus that common basic government functions such as citizen identity management need to be moved into a shared infrastructure in order to enable every government agency to tap into a common infrastructure rather than creating a one. In such a shared identity infrastructure model, electronic identity (e-Identity) cards are gradually becoming the means for service providers to identify and authenticate the service seekers with greater trust and confidence.

In such systems for National Identity Assurance, e- Identity cards and the associated credentials are generally subject to a number of different usage models over their lifecycle. This lifecycle is comprised of four stages:

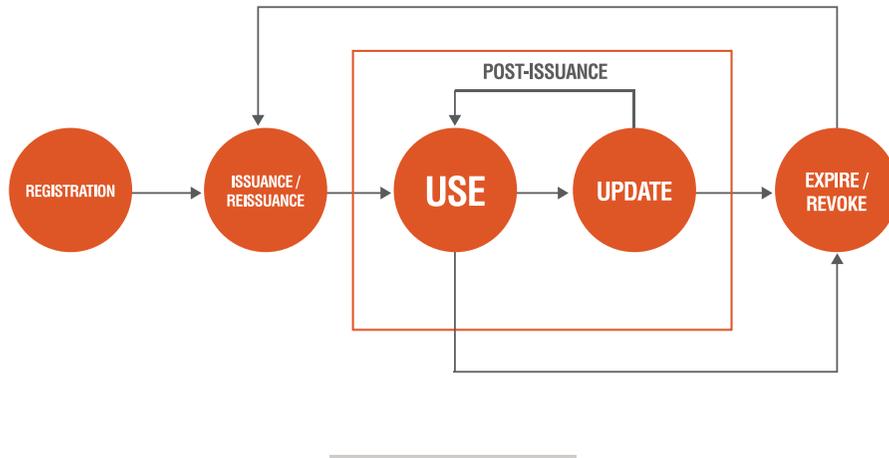


Figure 20: Credential Lifecycle

➔ **Registration:** The strength of the trust relationship depends upon the integrity of the how user identity is registered. Rigorous checks are made to ensure that a credential is issued to the correct individual.

➔ **Issuance/ Re-issuance:** This can be for first time issuance or re-issuance of the card after the expiry period or due to loss / damage.

➔ **Post-issuance:** Throughout its usage, trust and the credential must be maintained. This includes the monitoring and updating of the credential where necessary. This also includes the services required for organizations to use the e-Identity cards electronically.

➔ **Revoking:** For a trust relationship to maintain its integrity, it must become to an end in a controlled manner that is satisfactory to all parties. This applies equally to credentials, which must be revoked in accordance with the expectations of all stakeholders.

While e-ID card issuance is the beginning, the wide spread adoption of the e-ID is the key to unlocking its potential. The e-ID adoption rate is most likely driven by a broad range of factors that include:

- The underlying need, and readiness of the adoption community.
- The motivation to adopt the technology, which may include cost-savings or profits for users, mandatory/compliance issues, and the intervention by government or commercial providers to provide incentives for its adoption.
- Removal of barriers to adoption, which may include initial cost, the availability of tools such as Software Development Kit (SDK), ease of use, cultural acceptability and/or the consumer understanding of the need.

The compulsory use of a national identity that serves as an e-Identity also leads to the take-up rate of an e-Identity can being that much higher. A faster take-up means that the government can begin to start reaping the benefits more quickly of an e-Identity system, such as more efficient citizen-government interactions (Castro 2011). This faster return on investment means that these governments have more of an incentive to invest in an e-Identity program.

Many of the benefits from e-Identity stem from the effects of a positive network, thus the benefits grow as the number of user's increases. To illustrate this network effect, consider email, where the value of the email service to each user increases with the number

of users. The same is true for applications such as secure email, which require digital certificates; again, the value of the application increases as more users gain access.

6.4 Electronic identity (e-Identity) as a Key Enabler in E-Governance

In general, to favour the e-government uptake, special attention should be paid to the following issues: electronic transactions, electronic signatures and authentication, data protection and privacy, consumer protection, computer crime, and information security at large (United Nations Conference on Trade and Development 2012). Electronic Identity (e-Identity) cards provide an effective solution with which to address the above issues and enable e-governance.

The use of electronic identity, as the key enabler for e-governance, is a fact widely recognised by global institutions. Many of the international reports and surveys have started to incorporate new indicators that include the maturity as well as the availability of key enablers, such as e-Identity, interoperability guidelines, open standards and single sign-on features (Andreasson 2012). In 2010, the e-government action plan of the European Union (EU) identified interoperable electronic identification management (e-Identity) for access to public services and electronic document authentication as key enablers for e-government. (Commission of the European Communities 2006).

The effective use of an identity management system can help reduce costs, improve the quality of service delivery, drive the emergence of new integrated services and foster a service-oriented IT economy. Therefore, the key goal is to research, define and implement an identity management framework that is based on a secure and interoperable verification and authentication of identities. This makes the underlying identity technology - whether it is based on smart cards or on other security devices or biometric attributes - transparent and invisible to the application.

For example, the EU e-card strategy for the harmonization and consistent usage of smart cards envisages digital signature interoperability, which should be ensured through the adoption of accepted standards, authentication and encryption technologies. All e-Identity cards must permit the inclusion of the qualified digital signature at the time of issuance or at a later time, and all administrative procedures requiring a qualified signature must support the specified standards (Fioravanti and Nardell 2008).

E-Identity card holders can leverage it to authenticate government portals to avail themselves of public services. After being authenticated on a web-site or portal, the user may find it useful for being able to make statements or sign contracts in a way that is legally binding. Electronic signatures were developed to solve this kind of requirement. Similar to real life, the e-signature must not only contain information about the signatory, but it also must be trustworthy. Being able to authenticate and to electronically sign documents while connected to the Internet is what builds up the concept of electronic identity (Bour 2013).

E-Identity systems generate a variety of benefits for individuals, businesses, and government, which include facilitating commerce in the digital economy, enabling e-government services, and improving security for online transactions.

Many types of e-commerce transactions become more efficient with an e-Identity system. These systems enable individuals to authenticate within online services, securely communicate online, and create legally-binding electronic signatures, such as signing a contract or enrolling in a service. Businesses can also use identity management functions to interact with their customers, such as authenticating users of online applications.

Citizens benefit from electronic identity systems, which enable single-sign on (SSO). SSO gives individuals a more seamless online experience by allowing them to use one credential to sign in to multiple sites rather than having to log in multiple times using different credentials. The use of e-IDs also enables many private-sector services that depend on knowing the identity of the individual or something about the individual, such as his or her age, which is otherwise difficult to verify remotely. Some e-Identity can also be used as a digital wallet to make purchases both in person and online.

The use of e-Identity can also facilitate many types of e-government services. Government can streamline many services, such as providing government benefits, which depend on knowing an individual's identity. Also better innovative services can be offered such as online voting, that require remote authentication. Citizens may complete and sign government forms electronically from

anywhere with an Internet connection, which thus eliminates time-consuming trips to government offices or public notaries.

Similarly, businesses can also securely interact with the government online, for activities such as paying taxes or requesting permits. Using a secure electronic communication also eliminates the need to transcribe data from paper forms, which helps reduce errors as well as the processing time. An e-government can, therefore, receive many benefits from its increased efficiency. For instance, by eliminating duplicate data entry, as well as reducing the costs associated with unnecessary paperwork, which include the printing costs, storage, transportation and disposal.

Use of e-Identity systems can improve the security of online transactions and help prevent fraud and identity theft. First, e-Identity can create more trust and accountability in the identity ecosystem. For example, by creating sufficient audit logs, it may be possible to create chains of trust that allow a source of fraudulent e-Identity to be identified much more easily than with analogue IDs. Second, e-Identity can make it more secure for users to login to information systems by enabling multi-factor authentication. An example of multi-factor authentication would be: the user is required to have a PIN and have an e-Identity token to login to a website. Much like an ATM card, if an e-Identity is lost or stolen, it cannot be used without the PIN or password. Most information systems today do not use multi-factor authentication for user login. Instead, most users have to track and maintain multiple usernames and passwords with difficulty.

Although the best practice is to use a unique password for different accounts, individuals commonly reuse the password on multiple sites. This means that if a user's password is compromised on one website, it will be compromised on every other site that uses the same password; as well as locate and track every account that reuses this password. In contrast, when using an e-Identity, the user only has to change the password once. In addition, today, since users must remember multiple passwords, they often use a weaker, but easier-to-remember, password rather than a stronger, more complex, password. If users only have a single e-Identity to manage, they will have more of an incentive to use strong passwords.

6.5 Important E-Identity Services that Accelerate E-Governance Transformation

E-Identity services aimed at accelerating an e-governance transformation need to meet the following criteria:

- Provide integrated and standardized person identity services.
- Provide the infrastructure for the verification, management and tracking of socio-economic benefits delivery through the use of a national identity card.
- Provide services to manage the post issuance life cycle of the national identity card that include a centralized database

of hot listed cards and the services to facilitate card verification by the stakeholders.

- Provide centralized services to load, upgrade, activate and deactivate the card applications.
- Provide an online CRM through which the stakeholders can raise various issues related to the national identification system, which would be attended to and solved by the respective departments in a time bound manner.
- Provide the secure management of cryptographic keys.
- Facilitate the definition of Service Level Agreement (SLA) parameters and track the SLAs and the automated management of exception reporting and escalation chains.
- Provide improved levels of authenticity and accountability.

The following are some of the key e-identity related that are necessary to enable and accelerate any e-governance transformation:

Table 3: Key E-Identity Services to Enable and Accelerate E-Governance Transformation.

Service	Description
Open Certificate Status Protocol (OCSP)	An exposed PKI service that can be used to support online OCSP validation. OCSP can provide real time certificate status information. It supports the retrieval of certificate status information through various mechanisms including LDAP, CP, HTTP and most importantly through the direct integration with Certificate Authority databases.
Signature Validation	A service that can provide signature validation which includes certificate status validation. It relieves PKI-enabled applications from implementing the complex logic required to perform this action. This service performs the validation of digital signatures according to configured validation policies. It can perform certificate status checks against OCSP as well against CRLs.
Card Validation	An exposed service that can be used to provide on-line 'card validation'. Card validation checks the authenticity of an identity card in addition to PKI and the biometric authentication using the identity card.

Card Update	A service enabling card updates from any access point. This can be a simple data update from the identity provider or can be a complicated transaction that involves an application provider loading a new application on to the card.
PIN Reset	This service provides the ability to reset a PIN using an alternative method of authentication for example - biometric.
Authentication Service	This service is normally offered at the federal level and can be leveraged by all government agencies to authenticate e-Identity card holders and provide Single Sign On (SSO) to multiple government portals. Most of the current implementations provide support to standards such as SAML 2.0.
Electronic Notarization	This service provides trusted time-stamping and electronic attestation of documents, which is a foundation legal validity for critical documents such as Power of Attorney (PoA).

6.6 GCC National Identity Management Systems – A Case Study

GCC countries are at the forefront of countries around the world that are fast adopting smartcard based national identification systems. The main motive behind this transformation is to improve

the efficiency and effectiveness of service delivery as well as give social benefits to the population based on their entitlements. A national identification system can be used by both government and businesses to securely store and retrieve information about citizens and residents. Hence, it becomes an authentic source for verifying identities, and also their entitlement for benefits.

GCC countries have been promoting the adoption of the new smart cards with various initiatives. Their strategic intent is to simplify government service delivery and facilitate e-services and transactions; with a clear vision to make the new card an integral part of citizens' and expatriates' transactions with the government and private sector. The strategic objectives are illustrated in Table 4 below.

Table 4. The strategic Objectives of Identity Management Systems in GCC Countries

Priority	#	Strategic Objective	Strategic Intent
Primary	1	Enrol and maintain a current population register.	Contribute to national and individual security.
Secondary	2	Develop a secure, and integrated data access and exchange infrastructure.	Simplify government service delivery and facilitate e-transactions.



Figure 21: The GCC Smart ID Card Capabilities

The cardholders, be they citizens or expatriates, play different roles in different capacities - citizen, employee, customer, partner in various permutations and combinations. Within these roles, the identity card will act as the unified vehicle to prove the card holder's identity to the government and businesses as required. It is envisaged that the new smart identity card will act as the last mile enabler for e-governance initiatives in the GCC countries to provide an integrated platform for the citizens and expatriates to interact and transact online with various government and non-government agencies. Furthermore, new and innovative applications may evolve to augment the potential of the card for the advancement of civic life in the GCC countries.



Figure 22: Card Holder Roles

The GCC smart identity cards, with the combined strengths of PKI, smart card and biometric technologies, have created a robust and reliable identity system.

The GCC national identification systems offer the following benefits to the stakeholders:

- ➔ The smart card and PKI based National identity card greatly enhance and unify the identification and the verification capabilities thus replacing multiple redundant identification documents;
- ➔ The capability of generating a fool proof digital signature and, when used alongside biometric authentication, provides a high level of accountability and legal validity required for e-government and business transactions;

- The protection of personal data and PKI private keys on its chip.
- Enable the automation of business processes by eliminating the overhead of manual processes and paper work.

Based on these capabilities, the GCC countries intend to achieve the following objectives to enable e-governance transformation:

1. Improve operational readiness

- Provide federated identity services to enable the identification, authentication and electronic transactions.

- Assist cardholders and user organizations to overcome identity card adoption and usage hurdles.

2. Improve identity card adoption readiness of user organizations

- Continuously improve and innovate the identity card toolkit to make it the most robust and friendly interface to enable identity card adoption;
- Spread awareness and popularize the toolkit and its benefits;
- Enable the exponential scale value innovation of new breed solutions around the toolkit;
- Build technology demonstrators and killer applications to showcase the true potential of the identity card; and
- Build a highly skilled talent pool to innovate and support the identity card toolkit.

6.7 Role of Post-Issuance Identity Adoption Standards and Technologies

As discussed in the earlier chapters, electronic identity (e-ID) programs are a key enabler for e-government transformation. It consists of three stages, namely:

- Pre-issuance
- Issuance and,
- Post-issuance

‘Pre-issuance’ is service intensive and includes activities such as citizen enrolment, the registration of individual biometrics, and the verification of supporting documents etc. During this phase, a core identity service infrastructure such as population database etc. would be setup. Identity tokens, such as smartcards, as in most of the e-Identity programs, are issued during the phase called ‘Issuance.’ During this phase, e-Identity cards are printed, personalized with the information gathered during enrolment and finally dispatched to the card holders.

The objectives of the various e-Identity programs that exist today indicate that the aim of investments lies not in just issuing an e-Identity token such as a smartcard. Instead, the e-Identity is supposed to be leveraged at all the service delivery points that interact with citizens. Hence e-Identity adoption is a massive effort. From this, we can infer that the market size for post-issuance e-Identity adoption solutions is many times that of the identity card issuance itself.

This field is currently dominated by system integrators, which offer custom solutions that result in a high fragmentation of the market as well as a lack of standardisation. System integration also invests a huge effort in each custom solution deployment, which ultimately lowers their profitability. Being able to achieve a high degree of standardization is essential for sprouting innovations around the e-identity program.

Investing in the pioneering efforts in the Post-Issuance arena is the right answer to achieve the standardization of the e-identity adoption methods that would not only accelerate the adoption of modern identification systems to the fullest extent and so transform the public service delivery, but they would also generate high export potential as governments worldwide embrace electronic identification systems as well.

6.8 The Last Mile Enabler for the E-Governance Transformation in GCC Countries

GCC smart identity cards with all their function features contribute strongly to the e-government transformation and furthermore, more importantly contribute to their succeeding in accelerating the transformation efforts. The smart identity card seeks to be ‘the last mile’ enabler for this transformation.

With the support provided by the national identity issuing authorities, enterprise level e-Identity integration is enabled along

three dimensions:

- Identity information and credentials validation.
- Enterprise systems and applications integration.
- Identity as a service.

Today, users acquire multiple identity and credentials from enterprise systems and third party identity providers such as the national identity authority, and certificate of authority (CA) etc. To support these diverse credentials of users, organizations need to integrate them into the enterprise systems. This is complicated by the technical diversity of credentials and the diverse interfaces provided by different applications. Moreover, incorporating any change into the system is exponentially complex as it impacts every integration point. The diagram below depicts the complexity of point to point integration.

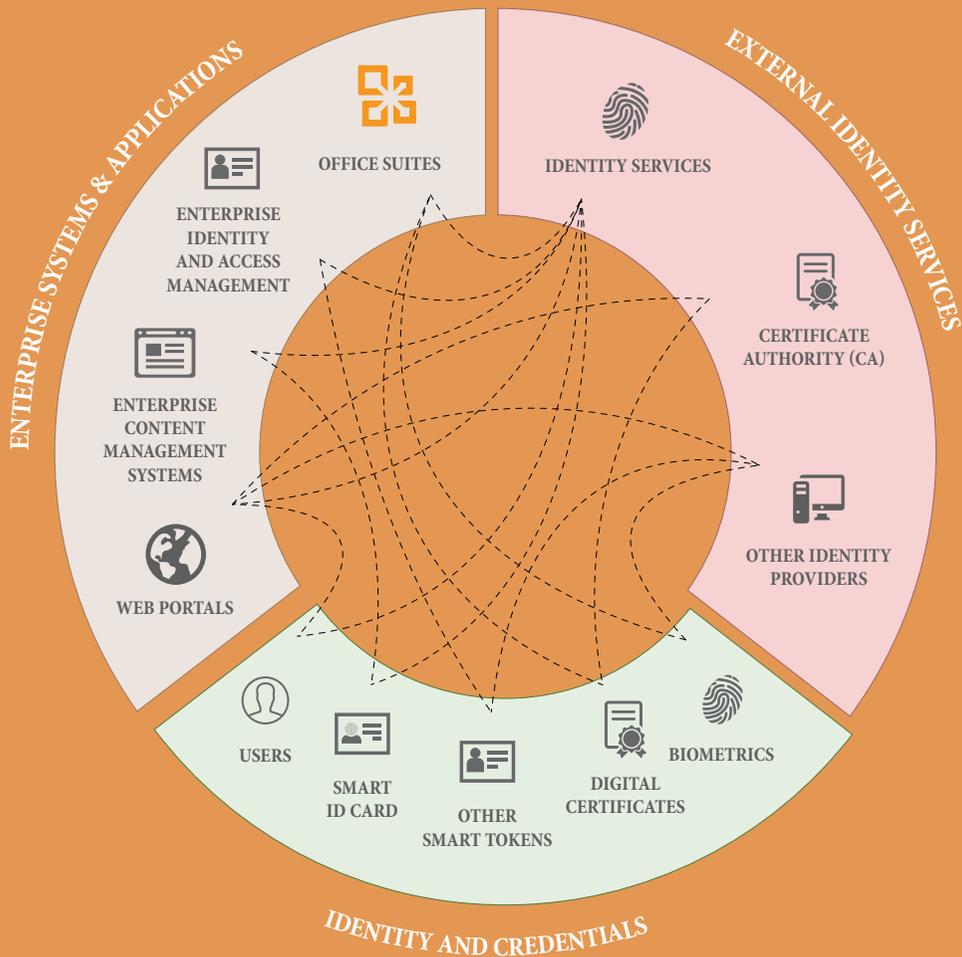


Figure 23: Complexity of Identity Systems Integration

6.8.1 Streamlining the Integration

The need of the hour is to generate a generic and standard method by which to overcome the complexity and the overhead involved in the current approach of e-Identity adoption. Some of the lessons can be learned from the e-Identity standardization drive initiated in the European Union (EU) under the umbrella of the European Citizen Card (ECC). The following diagram depicts the approach for a seamless integration of an identity card with enterprise systems and processes.

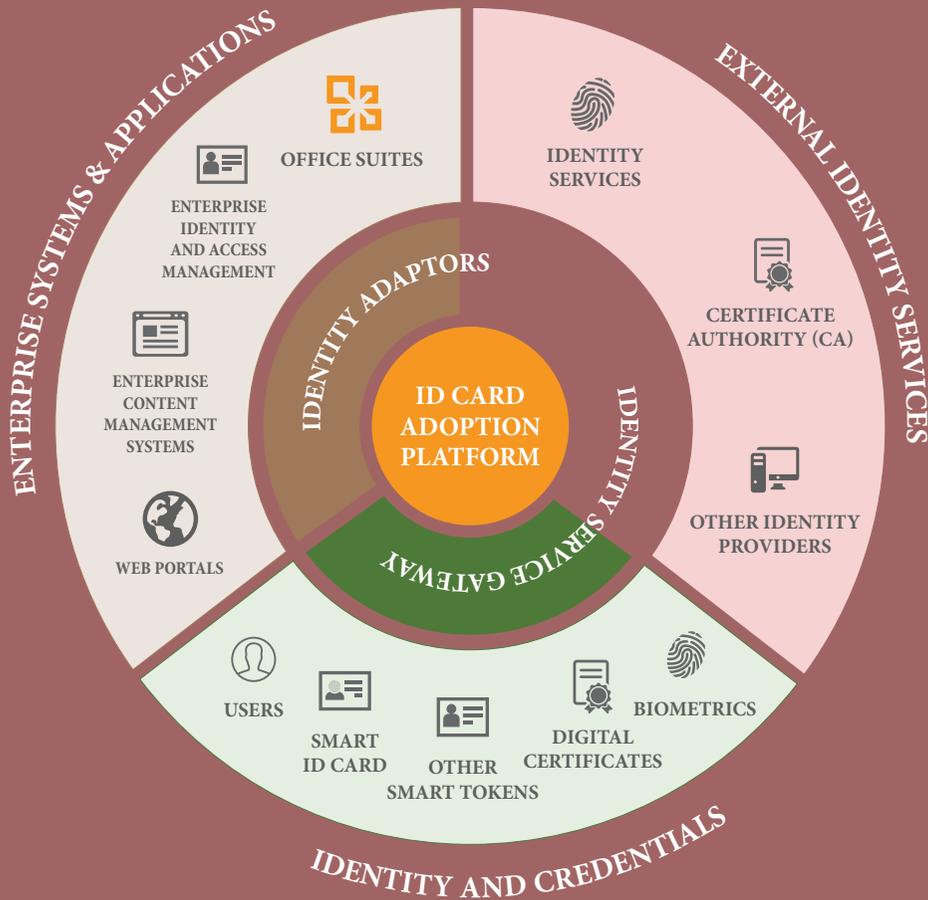


Figure 24: Solution for Streamlining Enterprise Identity Integration

The e-Identity adoption platform is envisaged to be provided by the issuing authorities in the GCC countries in the form of a National Validation Gateway and is supported by the global standards in the area of identity and credential management in order to achieve maximum interoperability. This National Validation Gateway is characterized by:

1. A generic interface and methods to capture, store and process identity information and credentials: This is addressed by generic and standardized interfaces. Behind the generic and standard interface of the gateway are connectors that integrate with external identity services through connectors that support various protocols such as OCSP, SOAP, TLS, LDAP and SAML. In the post-issuance e-Identity adoption scenario, this would be the single point interface for an enterprise to consume external identity and credential services.
2. Generic interface and methods to interact and consume external identity and credential services: This is addressed by the standardised identity card adoption platform provided by the SDK/ Tool Kit that is distributed freely by the governments. This is supported by multiple credential plugins that integrate with credentials through a diverse set of standards such as PCSC, ISO 7816, PKCS#11, PKCS#15, Microsoft Crypto API, and CT API, etc. identity card adoption platform is envisaged as an enabler for e-Identity throughout the IT system within an enterprise. This platform can also catalyse innovations of 'off the shelf' ready to use generic applications commonly used in enterprise that enable users to enjoy the benefits of

e-Identity directly in their popular software applications.

3. A generic e-Identity enabled enterprise application platform: This is to help system integrators develop their custom solutions development faster and easier with an enterprise application platform that offers various adapters to enterprise systems. This application platform is envisaged to provide all the identity and credential capabilities that are required for today's enterprise applications and portals with the help of an identity card adoption platform and identity services gateway. This platform should support SOA standards, JBI, XML, BPEL etc.

6.9 The GCC E-Identity Interoperability Model

The following diagram is a conceptual model for the e-Identity adoption in the GCC countries, which could pave the way to a federal level identity interoperability.

In this model, there are external identity providers and services that issue various credentials to the citizens, which are supposed to be leveraged by various government agencies and businesses. Leveraging the credentials means the integration of the credentials within various enterprise systems and business processes.

As depicted in the diagram, today, huge gaps exist between the identity issuers and the identity consumers. These gaps result from

a lack of common standards and technology platforms that could facilitate the smooth integration of these credentials. Thus, a need exists to integrate the core identity and credential services between the enterprises and the identity providers in order to facilitate identification, digital signing and verification, and transaction management.

Once the core identity adoption framework is in place, solutions are needed to integrate with the enterprise applications and business processes. This enterprise application platform should support identity integrated workflows, data exchange services, SLA and policy management. From this, we can model generic solutions such as over the counter (OTC) services and self service. This can be applied further to sector specific applications in banking, healthcare, education, government etc.

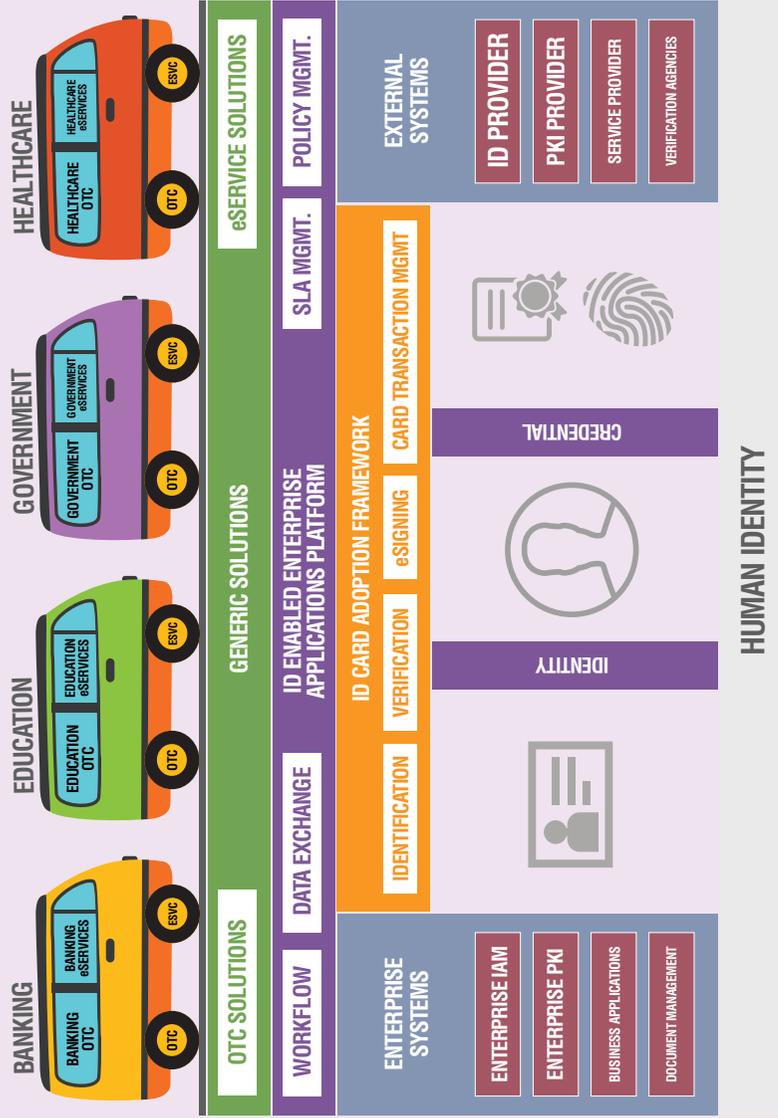


Figure 25: Conceptual Model for e-ID Adoption

6.10 M-Government and Mobile ID

What then does the government of the future look like? Well, it is one that works 24/7 and 365 days a year. It is as hospitable as a hotel, fast as a speeding bullet in delivering its services and strong in its accurate procedures. It is also innovative and adaptive and not only improves the quality of life, but as well, it helps people achieve their happiness. The GCC countries have started working on this vision and have recently launched the ‘m-Government’ project with the goal of providing government services via smart phones.

Through m-Government, the government aims to reach its people directly. Through its citizens, a smart phone government can make their lives easier. This project of m-government is expected to be completed within two years and the GCC governments are committed to implement the m-Government strategy.

To realize the m-government vision, mobile identification and authentication technologies play the key role in establishing trust between the citizen and the service providers. To facilitate this, the GCC countries have initiated mobile identification (Mobile Identity) strategies. The overall GCC strategy for mobile identity is depicted in the following diagram.

In the current GCC identity cards ecosystem, the identity card is issued with a smart chip as the secure element. The security features in the identity card include PIN protection, Public Key Infrastructure with asymmetric key encryption (Public Key + Private Key), digital certificates-identification as well as digital signatures and biometrics for in-person authentication.

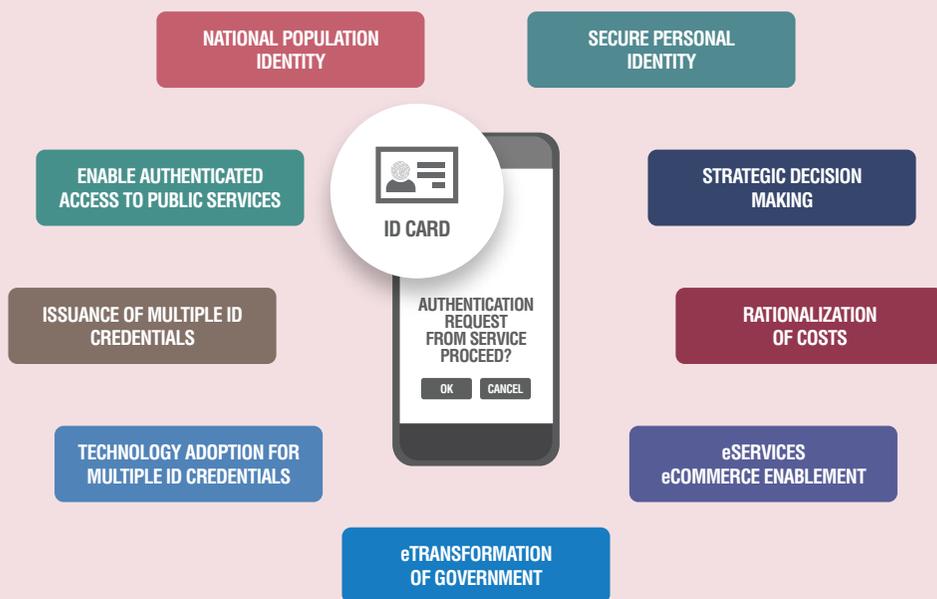


Figure 26: UAE Identity Mobile Strategy

whereas, in the proposed mobile identity strategy, the SIM card would be issued by a partnering telecom provider against the national identity card. In this scenario, a SIM card is used as the secure element. It is proposed to have the security features of Identity-PIN (Protection). Mobile Public Key Infrastructure with asymmetric key encryption (Public Key + Private Key), digital certificates-identification and digital signatures and digital signature for out of band hand authentication.

6.11 Value Innovation Strategy Built Around Smart Identity Cards

The main aim of value innovation centres focuses on increasing citizen convenience through accelerated service delivery. For the service provider, the costs of access management and the cost of delivery are reduced significantly.

Having seen the models and strategies for the realization of the citizen inclusive vision that can be realized through the identity card integrated delivery of e-government applications (CIVIC IDEA); it is clear that the goals of such great magnitude cannot be achieved in one go. We need to have carefully planned phases - each one built on the previous one that achieves a set of goals, and thus move steadily closer to the vision of the e-government transformation.

6.1.1.1 Stages of CIVIC IDEA Realisation



Figure 27: Stages of CIVIC IDEA Realization

The 'enable' stage is more of an elementary phase where the foundations for transformation are laid. At the 'enhance' stage, blue prints, standards and basic infrastructure evolve. Having created the basic infrastructure, goals have to be 'established' through smart projects to gain wider support and visibility which in turn creates demand. All through the first three phases, the overall strategy evolves through various phases and is now ready for 'expansion' to reach maximum coverage.

Having looked at the stages of the CIVIC IDEA realization, let's look at an approach to drive through these stages.

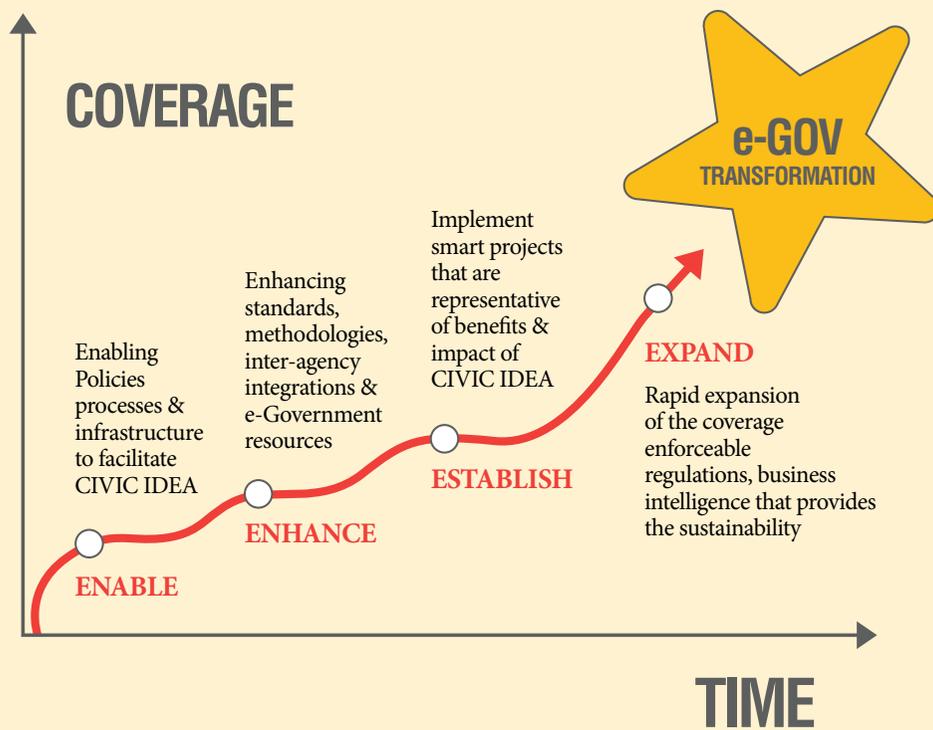


Figure 28: Growth Distribution across CIVIC IDEA Phases

The above diagram depicts the approach to drive through the four phases, with each phase expanding the coverage that encompasses services and end users. The 'enable' phase enables policies, processes and infrastructure to facilitate the CIVIC IDEA. The 'enhance' phase focuses on enhancing standards, methodologies, inter-agency integrations and e-governance resources. The 'establish' phase's prime focus is on implementing smart projects that are representative of the benefits and impact of the CIVIC IDEA. The 'expand' phase aims at the rapid expansion of coverage, enforceable regulations and business intelligence in the light of sustainability. The above discussed four phase model enables time bound, effective and dependable e-governance transformation.

6.11.2 Dimensions of the CIVIC IDEA

The realization of the e-governance transformation is at the intersection of top down and bottom up approaches, as depicted in Figure 29. At the very top, the government has to drive regulatory rights and laws towards enforcement and foster public private partnerships. Awareness, branding and human resource development to manage the e-governance resources becomes imperative. The creation of the infrastructure, which includes delivery channels, service access points and support mechanisms will bridge the delivery gap. This entire mechanism requires standards and guidelines; reviews and co-ordination mechanisms; and, project management and KPI monitoring.

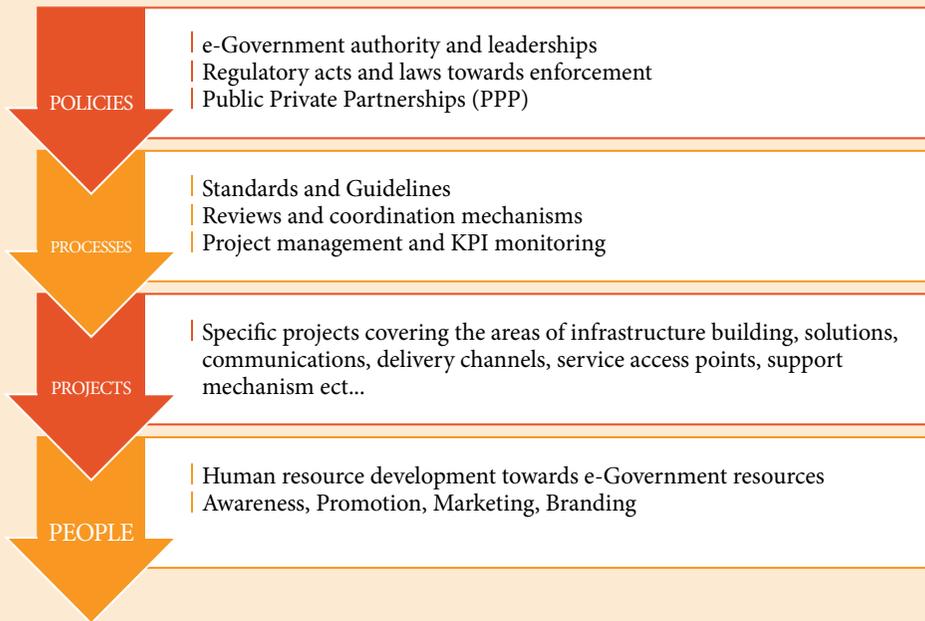


Figure 29: Dimensions of CIVIC IDEA

6.12 Conclusion

As we have seen, trust is the most important and intrinsic foundation on which e-government needs to be built. Electronic identification and the associated technologies like smartcard, PKI and biometrics can become the strong enablers for accelerating e-governance transformation. The use of modern and sophisticated electronic identification systems (like the e-Identity initiatives) is at the core of the e-government strategy in GCC countries, which along with the envisaged federated identity services is expected to propel these countries into becoming the nations with the most advanced e-governments.

7

EPILOGUE

7. EPILOGUE

E-government as a field is well established worldwide. Since the advent of the Internet, many maturity models were developed to better understand e-government evolution. The six-stage maturity model depicted in Figure 30 is a practical guide to examine e-government development stages:

1. **Inform** (establish an e-presence that provides information about the government/ department activities);
2. **Interact** (allow people and other stakeholders to interact by email, chat, call centres, web portals, social networking media and other channels);
3. **Transact** (enable people and other stakeholders to conduct transactions such as remote applications, request for services, service delivery on-line using all the interaction channels);
4. **Integrate** (where government departments are integrated at the backend to provide a seamless navigation and service-seeking, service bundling, shared services across government departments provide a rich user experience);
5. **Involve** (where people get involved in the governance - e.g. enabling e-voting, referendums, voicing public opinion, influencing the government decision making and optimizing the government departments to become 24-hour Authorities);
6. **Empower** (where citizens are empowered and protected legally and derive social benefits pro-actively).

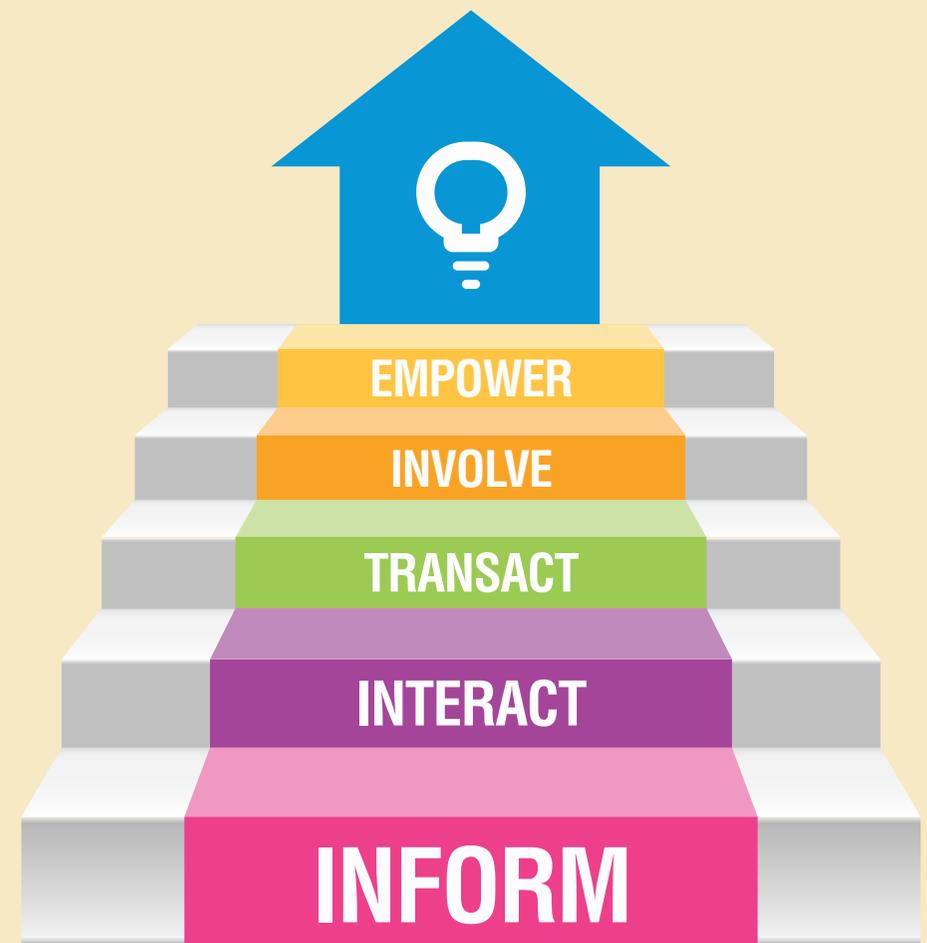


Figure 30: E-Government Transformation Model

What we are talking about in this context is e-transformation and more importantly accelerating this e-transformation. To achieve this we may well require a different mindset, perhaps through the use of a Blue Ocean strategy!

» It is proposed that the Blue Ocean mindset be adopted to promote distinctive opportunity-based thinking and bring in an accelerated transformation.

» Current e-government initiatives and e-government transformation strategies are seen as Red Oceans. A Blue Ocean is thus needed to be created with a focus on transforming the government engine to deliver higher value at a lower cost.

» In this context, Red Oceans represent all e-government strategies and all departments as well as the allied industries in existence today.

» These have defined rules, regulations, boundaries, goals, objectives and implementation plans.

» Blue Oceans represent all industries NOT in existence today.

This undefined space, otherwise known as OPPORTUNITY was brought in by the Augmented Identity Ecosystem that would be established based on national digital identification systems.

The Blue Ocean strategy is all about 'value creation' and working in a hitherto non-existent space. Governments with their national identification programs are perfectly poised to create this Blue Ocean bringing in an innovation that would create tremendous value to the digital and economic activity in the country. The e-government strategy achievement plans aligned with augmented identity in the form of digital identity profiles and credentials would contribute to the 'value innovation' leading to an enhanced citizen value proposition.

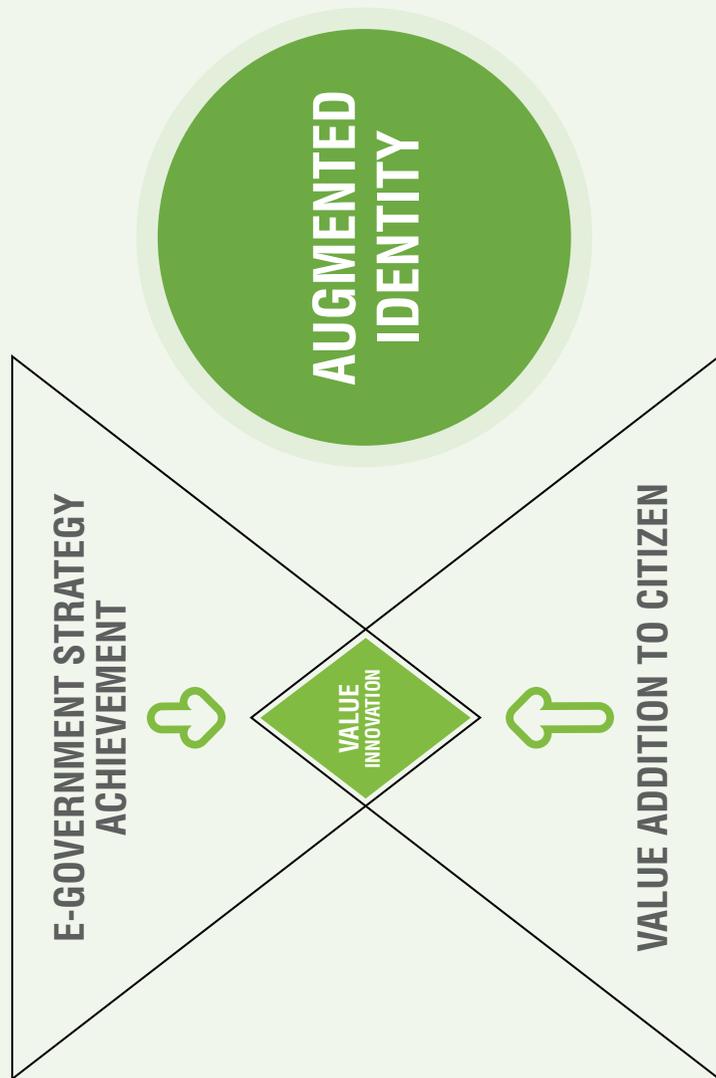


Figure 31: Augmented Identity

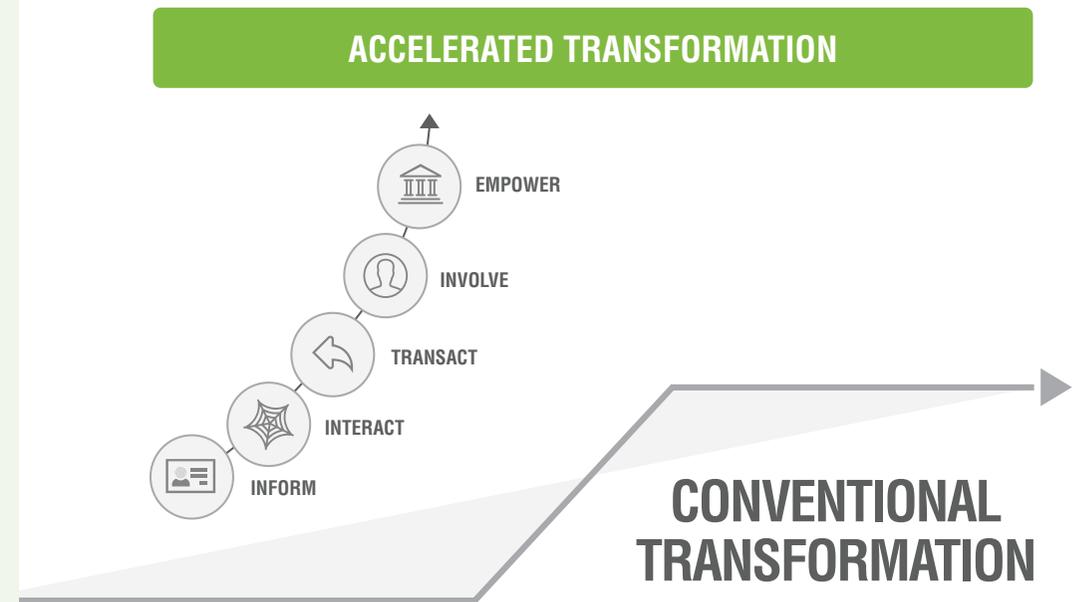


Figure 32: Conventional vs. Accelerated Transformation

The Blue Ocean Strategy for E-government Transformation Acceleration

Value innovation in e-government only occurs when government departments and business organizations align innovation with utility, price and costs. This ensures that all the stakeholders adapt to change and adopt the new technologies, and resources, drive down costs and in turn enhance their productivity.

The GCC countries are thus in the process of creating this Blue Ocean of opportunities. Secure smart digital identification systems

with personal identity credentials form the product offering that seeks to transform the landscape of economic activity in these countries.

The focus should be on both service differentiation and low cost in order to provide value to both citizens and business organizations such as government service providers and private service providers. The differentiation between the national identity from the existing personal identity system is undisputed. Efforts to provide National Validation Gateway for online identity verification and authentication can only further enhance the value proposition of identification systems in e-government transformation acceleration.

BIBLIOGRAPHY

1. AHN, Moon Suk. 2008. "Banishing Bureaucracy, Emerging E-government, and What Next?"" ICA 42nd Conference. Seoul, South Korea: International Council for Information Technology in Government Administration - ICA.
2. Al-Adawi, Z., S. Yousafzai, and J. Pallister. 2005. "Conceptual model of citizen adoption of E-government." The Second International Conference on Innovations in Information Technology (IIT'05).
3. Al-Khouri, Ali M. 2011. "An Innovative Approach for E-government Transformation." International Journal of Managing Value and Supply Chains.
4. Al-Khouri, Ali M. 2012. "PKI in Government Digital Identity Management Systems." European Journal of ePractice.
5. Al-Khouri, Ali M. and Malik Bechlaghem. 2011. "Towards Federated eIdentity Management across the GCC: A Solution's Framework." Global Journal of Strategies & Governance 30-49.
6. Al-Khouri, Ali M. and Naser M. Al-Mazrouei. 2010. "A Strategy Framework for The Risk Assessment and Mitigation for Large E-government Projects." IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.10, 29-34.
7. Andersen, Kim Viborg. 2006. "E-government: Five Key Challenges for Management." Electronic Journal of E-government 1-8.
8. Andreasson, Kim . 2012. "2014 UN E-government Survey: E-

government as an Enabler for Collaborative Governance." Overview paper in support of the Expert Group Meeting (EGM) in New York, USA, 4-5 December 2012. New York: UNPAN, 30 November.

9. Basu, Subhajit. 2004. "E-Government And Developing Countries: An Overview." International Review of Law, Computers & Technology 109-132.

10. Bour, Iona. 2013. Electronic Identities In Europe Overview Of e-ID Solutions Connecting Citizens To Public Authorities. UL Transaction Security. <http://www.ul-ts.com/downloads/whitepapers/finish/6-whitepapers/114-comparison-of-eid-solutions-with-privacy-preserving-characteristics>.

11. Brem, Alexander, and Kai-Ingo Voigt. 2009. "Integration of Market Pull and Technology Push in The Corporate Front End and Innovation Management—Insights From the German Software Industry." Technovation 351-367.

12. Brown, David H, and Sheryl Thompson. 2011. "Priorities, Policies and Practice of E-government In a Developing Country Context: ICT Infrastructure And Diffusion In Jamaica." European Journal of Information Systems 329-342.

13. Bughin, Jacques, Michael Chui, and James Manyika. 2010. "Clouds, Big Data, And Smart Assets: Ten Tech-Enabled Business Trends To Watch." McKinsey Quarterly (McKinsey & Company).

14. Bygstad, Bendik, Gjermund Lanestedt, and Jyoti Choudrie. 2007.

“Service innovation For E-government: A Broadband-Based Example.” *Electronic Government, an International Journal* 314–325.

15. Campbell, Jesse, and Tobin Im. 2012. “Beyond Ubiquity: Mobile Government, Theory And Practice.” KAPA conference at Seoul National. Seoul.

16. Castro, Daniel. 2011. *Explaining International Leadership: Electronic Identification Systems*. The Information Technology & Innovation Foundation - ITIF.

17. Chan, W., and Renâee Mauborgne. 2005. *Blue Ocean Strategy: How To Create Uncontested Market Space and Make Competition Irrelevant*. Harvard Business Press.

18. Chen, Alexander N., and Yumei Chen. 2009. “Critical Success Factors on E-government Application-From the View of Government Workers in Guangdong.” *Proceedings of the Ninth International Conference on Electronic Business*.

19. Cheng, Li-hung, Chao-tung Wen, Eldon Y. Li, and Ta-yi Lin. 2012. “Service Innovation Activities In E-Government Initiatives: The Taiwan Experience.” *International Journal of Services Technology and Management* 54–71.

20. Colesca, Sofia Elena. 2009. “Understanding Trust In E-government.” *Inzinerine Ekonomika-Engineering Economics* 7-15.

21. Commission of the European Communities. 2006. *i2010 eGovernment Action Plan*. [http://europa.eu/legislation_summaries/in-](http://europa.eu/legislation_summaries/information_society/strategies/l24226j_en.htm)

[formation_society/strategies/l24226j_en.htm](http://europa.eu/legislation_summaries/information_society/strategies/l24226j_en.htm).

22. Cook, Grahame, Dr Mark Matthews, and Stephen Irwin. 2009. *Innovation in the Public Sector: Enabling Better Performance, Driving New Directions*. Canberra: Australian National Audit Office.

23. Cordella, Antonio, and Federico Iannacci. 2010. “Information Systems In The Public Sector: The E-government Enactment Framework.” *The Journal of Strategic Information Systems* 52-66.

24. Dais, Alexandros, Mara Nikolaidou, Nancy Alexopoulou, and Dimosthenis Anagnostopoulos. 2008. “Introducing a Public Agency Networking Platform Towards Supporting Connected Governance.” In *Electronic Government*, 375–387. Springer.

25. Dutta, Soumitra, and Beñat Bilbao-Osorio. 2012. *The Global Information Technology Report 2012: Living in a Hyperconnected World*. Geneva, Switzerland: World Economic Forum.

26. Federal Ministry of Economics and Technology - BMWi. 2010. *ICT Strategy of the German Federal Government: Digital Germany 2015*. Munich, November.

27. Fioravanti, Fabio, and Enrico Nardell. 2008. “Identity Management for E-government Services.” In *Digital Government*, 331-352. Springer.

28. Gall, Nicholas, David Newman, Philip Allega, Anne Lapkin, and Robert A. Handler. 2010. “Introducing Hybrid Thinking For Transformation, Innovation And Strategy.” *Gartner Research Identity*

Number: G00172065.

29. Ghana Government. 2009. eGovernment Interoperability Framework (eGIF). Ghana Government.

30. Gil-García, J. Ramón, and Theresa A. Pardo. 2005. "E-government Success Factors: Mapping Practical Tools to Theoretical Foundations." *Government Information Quarterly* 187-216.

31. Godin, Benoît, and Joseph P. Lane. 2013. "Pushes and Pulls": The Hi(story) of the Demand Pull Model of Innovation. Montreal, Quebec: Project on the Intellectual History of Innovation.

32. Guijarro, Luis. 2007. "Interoperability Frameworks And Enterprise Architectures In E-government initiatives in Europe and the United States." *Government Information Quarterly* 89-101.

33. Hite, Randolph C. 2004. *The Federal Enterprise Architecture and Agencies' Enterprise Architectures Are Still Maturing*. United States General Accounting Office.

34. Hossan, Chowdhury Golam, Md Wahidul Habib, and I. Kushchu. 2006. "Success and Failure Factors for E-government projects implementation in developing countries: A study on the perception of government officials of Bangladesh." *Proceedings of the 2nd European Conference on Mobile Government, Mobile Government Consortium International*.

35. Howell, Lee W. 2013. *Global risks 2013*. Geneva, Switzerland:

World Economic Forum.

36. Karokola, Geoffrey, and Louise Yngström. 2009. "Discussing E-government Maturity Models for the Developing World-Security View." *ISSA*. 81-98.

37. Koch, Per, and Johan Hauknes. 2005. *Innovation in the Public Sector*. Oslo: PUBLiN.

38. —. 2005. *On innovation in the public sector*. NIFU.

39. Kushchu, Ibrahim, and Halid Kuscu. 2003. "From E-government to M-government: Facing the Inevitable." *The 3rd European Conference on E-government*. 253-260.

40. Mossberger, Karen, and Caroline Tolbert. 2006. "The Effects Of E-government On Trust And Confidence in Government." *Public Administration Review*. American Society for Public Administration. 354-369.

41. Nabafu, Robinah, and Gilbert Maiga. 2012. "A Model of Success Factors for Implementing Local E-government in Uganda." *Electronic Journal of E-government* Volume 10 Issue 1 2012 31 - 46.

42. *National Performance Review - NPR*. 1993. *From Red Tape to Results: Creating a Government that Works Better and Costs Less*. Washington, DC: Government Printing Office.

43. Nemet, Gregory F. 2009. "Demand-Pull, Technology-Push,

and Government-Led Incentives For Non-Incremental Technical Change.” *Research Policy* 700-709.

44. Nicoll, Paul, Judi Robinson, and Brendan O’Hanlon. 2005. *Measuring the efficiency and effectiveness of E-government*. Canberra: Australian National Audit Office.

45. Novakouski, Marc, and Grace A. Lewis. 2012. *Interoperability in the E-government Context*. Carnegie Mellon University, Carnegie Mellon University.

46. Office of Management and Budget. 2012. *The Common Approach to Federal Enterprise Architecture*. The White House.

47. Olphert, C. W., and Leela Damodaran. 2004. “Dialogue with Citizens—the Missing Link in Delivering E-government?” *Proceedings of the International Conference on Politics and Information Systems: Technologies and Applications*, Orlando, Florida. Florida. 21–25.

48. Partnership on Measuring ICT for Development. 2011. *Framework for a Set of E-Government Core Indicators*. Economic Commission of Africa.

49. Prahalad, C.K., and M.S. Krishnan. 2008. *The New Age of Innovation: Driving Cocreated Value Through Global Networks*. McGraw Hill.

50. Rabaiah, Abdelbaset, and Eddy Vandijck. 2009. “A Strategic Framework of E-government: Generic and Best Practice.” *Electronic*

Journal of E-government Volume 7 Issue 3 (*Electronic Journal of E-government* Volume 7 Issue 3) 241 - 258.

51. Saekow, Apitep, and Choopol Boonmee. 2009. “A Pragmatic Approach to Interoperability Practical Implementation Support (IPIS) for E-government Interoperability.” *Electronic Journal of E-government*.

52. Saha, Pallab. 2010. *Enterprise Architecture as Platform for Connected Government*. UNPAN.

53. Schwab, Klaus. 2012. *The Global Competitiveness Report 2012-2013*. Geneva, Switzerland: World Economic Forum.

54. Shahkooh, Kolsoom Abbasi, Ali Abdollahi, Mehdi Fasanghari, and Mohammad Azadnia. 2009. “A Foresight based Framework for E-government Strategic Planning.” *Journal of software* 544–549.

55. Siddiquee, Noore Alam. 2008. “E-government And Innovations In Service Delivery: The Malaysian Experience.” *Intl Journal of Public Administration* 797–815.

56. The Government of UAE. 2011. “UAE National Charter 2021.” www.dubai.ae. www.dubai.ae/sitecollectiondocuments/uae_vision_2021_english.pdf.

57. Thenint, Hugo. 2010. *Innovation in the public sector*. *Global Review of Innovation Intelligence and Policy Studies - INNO GRIPS*.

58. United Nations Conference on Trade and Development. 2012.

Information economy report 2012: the software industry and developing countries. New York: United Nations Publications.

59. Valdés, Gonzalo, Mauricio Solar, Hernán Astudillo, Marcelo Iribarren, Gastón Concha, and Marcello Visconti. 2011. "Conception, Development And Implementation Of An E-government Maturity Model In Public Agencies." *Government Information Quarterly* 176-187.

60. West, Darrell M. 2004. "E-government and the Transformation of Service Delivery and Citizen Attitudes." *Public administration review* 15-27.

61. Wikipedia. n.d. Spacecraft Propulsion. http://en.wikipedia.org/wiki/Spacecraft_propulsion.

62. Wimmer, Maria A. 2002. "Integrated Service Modelling For On-line One-Stop Government." *Electronic Markets* 149-156.

63. World Scenario Series. 2007. *The Gulf Cooperation Council (GCC) Countries And The World: Scenarios to 2025*. Geneva, Switzerland: World Economic Forum.

64. World Scenario Series. 2007. *The United Arab Emirates and the World: Scenarios to 2025*. Geneva, Switzerland: World Economic Forum.

65. Wyld, David C. 2009. *Moving to the Cloud: An Introduction to Cloud Computing in Government*. IBM Centre for - The Business of Government.

66. Yu, Calvin Chun, and Paul Jen-Hwa Hu. 2007. "Rethinking the Relationship between Ubiquitous Government and Electronic Government." 11th Pacific-Asia Conference on Information Systems.

67. —. 2007. "Rethinking the Relationship between Ubiquitous Government and Electronic Government." 11th Pacific-Asia Conference on Information Systems. Auckland, New Zealand: Pacific-Asia Conference on Information Systems.

68. Zenghelis, Dimitri. 2011. *The Economics of Network-Powered Growth*. Cisco.

ACRONYMS

Acronym	Definition
Authentication	A process of determining whether someone or something is, in fact, who or what it is declared to be.
Biometric	Distinctive and measurable human characteristics that can describe individuals such as fingerprints, palm veins, face recognition, DNA, palm print, iris recognition, voice, etc.
Blue Ocean	A systematic approach that outlines principles and tools organizations can use to create and capture untapped opportunities.
Business Intelligence (BI)	Comprises strategies and technologies used by enterprises for the data analysis of business information.
Business to Business (B2B)	The exchange of products, services or information between businesses.
Business to Consumer (B2C)	A business or transaction conducted directly between a company and consumers who are the end-users of its products or services.

Change Management	A systematic approach to prepare and support individuals, teams, and organizations in making organizational change.
Citizen Charter	Represents the commitment of the Organization towards standard, quality and time frame of service delivery, grievance redress mechanism, transparency and accountability.
Citizen-Centric Government	An approach that promotes “citizens engagement” in the various phases of the service definition, development, refining and monitoring.
CIVIC IDEA	A model for the realization of the citizen inclusive vision that can be realized through the identity card integrated delivery of e-government applications.
Digital Certificate	An electronic document that allows a person, computer or organization to exchange information securely over electronic networks using the public key infrastructure (PKI).

Digital Economy	An economy that functions primarily by means of digital computing technologies, especially electronic transactions made using the Internet and related information and communications technologies. The term "digital economy" is intertwined with the traditional economy making a clear delineation harder.
Digital Identity Management	The process of identifying an individual or a machine within a network, application or system and controlling their access to resources within those systems and applications.
Digital Inclusive Society	Refers to the activities necessary to ensure that all individuals and communities, including the most disadvantaged, have access to and use of Information and Communication Technologies (ICTs).
Digital Signature	A mathematical scheme used to validate the authenticity and integrity of digital messages or documents.
Digital Society	A modern, progressive society that is formed as a result of the adoption and integration of Information and Communication Technologies (ICT).

Electronic Commerce (E-Commerce)	The buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet.
Electronic Government (e-Government)	The use of information and communication technologies (ICTs) to improve public sector organisations' efficiency, effectiveness, transparency and performance, with the end in view of fulfilling citizen needs. It aims transform internal operations to enhance the access to and delivery of government services to benefit citizens, business partners and employees and agencies.
Electronic Identity (e-Identity)	An electronic identification solution to enable access to benefits or services.
Electronic National Identity	An identity token, mainly comes in the form of a smart card with digitally-embedded information, issues as a means of confirming the identity.
Electronic Service (E-Service)	Refers to providing government services through the Internet or other electronic means.

Encryption	The process of encoding a message or information in such a way that only authorized parties can access it.
Enterprise Architecture (EA)	A conceptual blueprint that defines the structure and operation of an organization with the intent to determine how an organization can most effectively achieve its current and future objectives.
Government to Business (G2B)	The conducting of transactions between government bodies and business via the Internet or electronic means.
Government to Citizen (G2C)	The relationships between organizations of public administration and a citizens, e.g, online access to information and services.
Government to Government (G2G)	The electronic sharing of data and/or information systems between government agencies, departments or organizations.
Gulf Cooperation Council (GCC)	A regional intergovernmental political and economic union consisting of six Arab states: Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates.
Identification	Evidence of identity; something that identifies a person or machine.

Information and Communications Technology (or Technologies) – ICT	The infrastructure and components that enable modern computing.
Interoperability	The extent to which different information technology systems and devices can communicate, exchange data, interpret and use the data that has been exchanged.
IT Governance Framework	Formal guidelines and measures that provide a structure for organizations to ensure that IT investments support and enables the achievement of corporate strategies and objectives.
Mobile Government (M-Government)	A subset of e-government, that aims to make public information and government services available through mobile and wireless technologies like cellular/ mobile phones, and laptop computers, personal digital assistants (PDAs) and wireless internet infrastructure.
National Validation Gateway	An architecture built to provide secure online, real-time services related to validation, verification and authentication of E-Identity credentials.

Over the Counter (OTC)	An operation or transaction taking place between two parties requiring physical presence to complete it.
Public Key Infrastructure (PKI)	A technology that supports users and computers to both securely exchange data over networks (through encryption) and verify the identity of the other party.
Research and Development (R&D)	Systematic activity combining both basic and applied research that is aimed at discovering solutions to problems or creating new goods and knowledge.
Return on Investment (ROI)	A performance measure used to evaluate or compare the efficiency of an investment, mainly by measuring the amount of return on an investment relative to the investment's cost.
Service Level Agreement	A contract between a service provider and its internal or external parties that documents what services the provider will furnish and defines the performance standards the provider is obligated to meet.
Service Quality	An assessment of how well a delivered service conforms to perceptions and expectations related to specific dimensions namely reliability, responsiveness, assurance, etc.

Single-Sign On (SSO)	Is a property of access control that provides users to log in with single identities to gain access to connected systems.
Smart Card	A pocket-sized card with an embedded chip designed to be tamper-resistant and uses encryption to protect in-memory information, used in general to provide personal identification, authentication, data storage, and application processing.
Software Development Kit (SDK)	A set of software development tools that allows the creation of applications for a certain software package, software framework, hardware platform, computer system, or similar development platform.
System Integration (SI)	A process of bringing together different information systems into one system and ensuring that they function together as one system through developing a customized architecture or application.
United Nations Department of Economic and Social Affairs (UN DESA)	A United Nations entity tasked to promote and support international cooperation, and assist governments in agenda-setting and decision-making on development issues.

ABOUT THE AUTHOR



Dr. Ali M. Al-Khouri is the Chairman of the Arab Federation for E-Commerce; one of the international organizations of the Arab Economic Unity Council, League of Arab States with the mission to stimulate cross border e-commerce between Arab countries as well as globally. He is also a senior government official in the United Arab Emirates. With a total experience of over 25 years, he participated in many mission-critical and strategic projects implementation in the public sector. Besides, he is also a Professor and Fellow of the British Institute for Technology in London, UK, as well as a fellow and member in many scientific and research associations. He is further recognized both nationally and internationally as think-tank, and for his management expertise and technical knowledge, having developed different intellectual methodologies and frameworks to support various fields of practice. He has published over 100+ management books and scientific research articles in international peer-reviewed journals.



Head Office:

P.O.Box: 2692 Al Horreya Post Office,
Heliopolis – Cairo
Arab Republic of Egypt
Tel. No.: +(202) 2258 0006
Fax. No.: +(202) 2258 0077
E-mail: arado@arado.org

Regional Office:

Al Qasbaa Water Canal Al Sharjah
United Arab Emirates
Tel. No.: +(971 - 6) 5563 399
Fax. No.: +(971 - 6) 5567 007
E-mail: aradosh@arado.org

He served as an advisor to many national and international organizations and advisory boards of academic institutions. He joined the World Economic Forum councils on different workgroups, as one of the world's most relevant and knowledgeable thought leaders in various fields, and to support the Global Agenda Councils to deliver pertinent insights and collaboratively develop solutions to address major global challenges. He also served as a special advisor to European Union on STORK 2.0 project, and as an advisory observer to Identity Security Alliance in Europe.

Dr. Al Khouri attained his higher education from the top UK universities, where he received his B.Sc. (Hons.) in 'Business Information Technology Management' from Manchester University, M.Sc. in 'Information Management' from Lancaster University, and an Engineering Doctorate (EngD) from Warwick University in the field of 'Strategic and Large Government Projects Management'.



@dralialkhouri