e-GOVERNMENT INTEROPERABILITY: A COOPERATIVE ARCHITECTURE MODEL TO FACILITATE INFORMATION SHARING IN NAMIBIA

A THESIS SUBMITTED IN PARTIAL FULFILMENT
OF THE REQUIREMENTS OF
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

OF

THE UNIVERSITY OF NAMIBIA

BY

STEFANUS VAN STADEN

NOVEMBER 2011

Main Supervisor: Doctor Jameson Mbale (University of Namibia)

Co-Supervisor: Professor Alfredo Terzoli (University of Rhodes)

ABSTRACT

Governments face continued pressure to increase their performance with the aim to improve efficiency and service delivery to their stakeholders, customers and citizens. To improve efficiency and performance, Governments adopt e-Government models and Information and Communication Technology (ICT) solutions as enablers and vehicles for transforming public administration. As part of the transformational process, Public Services need to transform themselves into an integrated entity that responds to the needs of its stakeholders, customers and citizens.

Interoperability solutions provide the means for accomplishing integration by interlinking heterogeneous Information Systems and infrastructures that would allow data to be shared and exchanged within the Public Service. Interoperability is one of the most crucial barriers that e-Government initiatives should overcome. The study highlights the critical role of interoperability and presents a qualitative survey of technical interoperability and interoperability adoption factors within the Public Service of Namibia. It also proposes theoretical models that define and describe ways of establishing technical interoperability within the key areas of data, software and communications.

The study used a qualitative research approach of descriptive type in which explorative research was combined with case study research. As part of the explorative research process, literature study was carried out to clarify the different aspects (e.g., interoperability maturity, interoperability adoption factors) of interoperability and to identify distributed architectural forms available for establishing interoperability. Case study research was conducted to investigate the technical interoperability dynamics within the public service, so as to obtain a better understanding of the uniqueness and idiosyncrasy of technical interoperability among Information Systems and the factors that

may influence technical interoperability adoption in all its complexity. Data was gathered for Information Systems interoperability cases through semi-structured interviews from Public Service Information Technology (IT) Managers and IT Staff.

A quantitative analysis of the qualitative data collected from the different Information Systems interoperability cases were performed using Microsoft Excel and the MoonStats statistical software program. The analysis findings indicated that technical interoperability was limited to a small number of public service organisations and that technical interoperability between Information Systems was at a low level of sophistication and compliance. The analysis findings further indicated that there was a need to increase the level of technical interoperability sophistication and compliance between Information Systems and to further expand the number of technical interoperability Information Systems. The data analysis findings identified twenty-four factors that may influence the adoption of interoperability within the Public Service of Namibia of which ‘Data Security’ and ‘Data Quality’ were the most identified by respondents.

Based on the study findings and the supporting models developed, a conceptual Cooperative Architectural Model (CAM) was developed and proposed. The conceptual model provides technical interoperability guidance through a conceptual, layered and distribution architecture.

The study concludes that the conceptual Cooperative Architectural Model (CAM) proposed in this study meets the architectural requirements identified and serves as a conceptual architectural blueprint for achieving the desired state of technical interoperability within the Public Service of Namibia.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

CAM: Cooperative Architectural Model.

CIA: Confidentially, Integrity and Availability.

FTP: File Transfer Protocol.

MITU: Ministerial Information Technology Units.

HTTP: Hypertext Transmission Protocol.

ICT: Information and Communication Technology.

IIOP: Internet Inter-Object Request Broker Protocol.

IP: Internet Protocol.

IT: Information Technology.

G2B: Government-to-Business.

G2C: Government-to-Citizen.

G2G: Government-to-Government.

GIF: Government Interoperability Framework.

GIGF: Government Interoperability Governance Model.

GIGM: Government Interoperability Governance Model.

O/M/A: Office/Ministry/Agency.

OPM: Office of the Prime Minister.

ISIMM: Information Systems' Interoperability Maturity Model.

LAN: Local Area Network.

MOF: Ministry of Finance.

NEA: National Enterprise Architecture.

NPSCOIT: Namibia Public Service Committee on IT.

RMI: Remote Method Invocation.

RPC: Remote Procedure Calls.

SOA: Service Oriented Architecture.

SOAP: Simple Object Access Protocol.

TCP: Transmission Control Protocol.

UNAM: University of Namibia.

VSP: Vendor specific protocol.

WAN: Wide Area Network.

XML: Extensible Mark-Up Language Text Format.

ACKNOWLEDGEMENT

The writer wishes to acknowledge with gratitude the generous help and support received from my colleagues in the Department of Public Service IT Management within the Office of the Prime Minister who were willing to assess the various models developed and who were willing to share their expertise.

I would particularly like to single out my supervisors, Dr. Jameson Mbale for his expert inputs and his guidance to keep me focused on the task at hand when I was lost in a sea of ideas and information. I also thank Dr. Jameson Mbale for insisting that I should write Journal and Conference papers and the help that he provided to me in doing so.

I acknowledge my father, Stefanus van Staden, for the research methodology guidance and assistance provided throughout the study. I further would like to thank him for taking the time to review my thesis chapters and for his suggestions and corrections.

Thanks are also due to all the Public Service IT Managers and IT Staff that willingly offered their time to be interviewed. I would also like to thank them for the enthusiasm that they showed and the expert inputs provided.

Finally, I would like to thank the different committees at the University of Namibia (UNAM) for their corrections and suggestions in improving the presentation of this thesis. To everyone who helped directly and indirectly, I say thank you.

DEDICATION

To God Almighty, my wife Alida, my children Ancke and Gesie, my father Stefanus and my mother Susan.

DECLARATION

I, Stefanus van Staden, declare that this study titled "**e-Government Interoperability: A Cooperative Architecture Model to Facilitate Information Sharing in Namibia**" is a true reflection of my own research, and that this work, or part thereof has not been submitted for a degree in any other institution of higher education.

Full Name: **Mr. Stefanus van Staden**

Signature: _____

Date: _____

1. INTRODUCTION

The chapter introduces the research by providing an overview of the study topic, research problems, research aim, research questions, study scope, research methodology and summary of the findings. The chapter concludes with an outline of the chapters of the thesis and a chapter summary.

1.1 Introduction

Electronic Government (e-Government) reflects the final vision for Public Services and Governments that will allow them to undergo enormous modernization and reorganisation (United Nations Department for Economic and Social Affairs [UNDESA], 2008).

Broadly, e-Government can be defined as the use of Information and Communication Technology (ICT) to transform Government by making it more accessible, effective and accountable to citizens and its stakeholders (United Nations Educational, Scientific and Cultural Organization [UNESCO], 2005). e-Government covers the whole scope of administration, and is at the core of public management modernisation (Pankowska, 2008).

The success of e-Government requires that Governments fundamentally change the way they work and interact with citizens and stakeholders. The adoption of e-Government will require Governments to embrace ICT advancements to reduce operational costs, improve business processes, connect stakeholders, improve service delivery and realise the vision of good governance (UNESCO, 2005).

According to UNESCO (2005), the foundation of e-Government deployment within a Government is formed around four primary types of interactions, namely:

(a) **Government-to-Government (G2G):** G2G interaction involves the sharing of data and provisioning of electronic information exchange within the Government and with stakeholders. The sharing and exchange of data and information could be both intra governmental (i.e., within an agency) and inter-governmental (i.e., between agencies) as well as among external entities at local and national levels (ibid).

(b) **Government-to-Citizen (G2C):** G2C are interactions where electronic dissemination of information and provisioning of electronic services takes place. G2C also includes key components that would allow citizens to participate in the policy formulation process of government (ibid).

(c) **Government-to-Business (G2B):** G2B interaction focuses on increasing the efficiency of procuring practices and the sale of Government goods to the public. Further, this type of interaction involves electronic transactions and exchange between Government and business entities (ibid).

(d) **Government-to-Employee (G2E):** This type of interaction covers the provisioning of employee information and employee self-service transactional services (ibid).

To achieve the aims of e-Government, there is a need to connect Government (i.e., G2G, G2C, G2B and G2E) internally and externally to its stakeholders. The key concept that the connected Government is built on is that of interoperability (Pardo & Burke, 2008).

In its broad sense, interoperability is the ability of multiple diverse Government ICT systems or components to purposefully and seamlessly exchange information and use the information that has been exchanged (Lallana, 2008). Interoperable systems and components are linked together through some form of data exchange mechanism that will allow them to request and receive data and services from each other (Jolma & Rizzoli, 2003).

Government Interoperability allows diverse services and data offered by agencies to be linked, increasing the ease of information sharing among different agencies and enabling one-stop online services (Lallana, 2008). Government Interoperability emphasizes the ability of connected members to share knowledge and other resources in addition to creating interoperability infrastructure (Pardo & Burke, 2008).

To achieve a meaningful level of interoperability, a Government must be interoperable on at least three levels such as: (a) business level, (b) knowledge level, and (c) ICT level. In preparation for establishing interoperability between systems, interoperability should be analysed from views such as: (a) enterprise view, (b) architecture view, (c) platform view and (d) ontology view (Pankowska, 2008).

Interoperability can be achieved within the Government through the adoption of interoperability standards or architecture. Achieving interoperability through standards entails the adoption of a Government Interoperability Framework (GIF). The GIF is set of standards (e.g., reference and compatibility standards) and guidelines that are used to specify the method of interaction. Alternatively, interoperability could be achieved through a National Enterprise Architecture (NEA). NEA serves as a strategic planning framework that relates and aligns Government ICT with Government functions. NEA provides for common resources and defines the rules for their use and re-uses (Lallana, 2008).

The desirable future outlook of e-Government should cover new design methodologies and construction processes founded on interoperability frameworks and architectures (Lallana, 2008). e-Government requires an evolutionary and comprehensive architecture to avoid duplications of infrastructure and components and to integrate disparate administrative processes, services and activities (United Nations Department for Economic and Social Affairs [UNDESA], 2008).

In establishing interoperability, Government will be confronted by significant problems in managing and integrating autonomous, heterogeneous and distributed information sources and systems. At the heart of the interoperability problem lay the different ways to organise knowledge and information within different policy areas (Jolma & Rizzoli, 2003). Additionally, technical, syntactical, semantic and organisational interoperability issues will also need to be addressed in the process of establishing interoperability.

This study focussed on investigating and analysing the Public Service of Namibia's technical interoperability state and defining suitable theoretical solutions to establish technical interoperability within the Public Service.

1.2 Statement of the Problem

Since independence, the Namibia Public Service is faced with a number of challenges on how to improve public management and the quality of service delivery. In an effort to exploit the potential offered by Information Technology (IT) towards improving decision making and service delivery, the Namibia Public Service Committee on IT (NPSCOIT) formulated the Information Technology Policy for the Public Service in 1993.

The Information Technology Policy for the Public Service permit's Offices/Ministries/Agencies (O/M/As) to establish Ministerial IT Units (MITUs'). The MITUs' are responsible for planning, budgeting, developing, implementing and maintaining computer systems for their organisations. In accordance with the principles of division of powers, sectorial Information Systems will be independently administered by public service organisations in their assigned area of administration (Namibia Public Service Committee on IT [NPSCOIT], 2004).

The Information Systems development activities undertaken by MITUs' are generally based on a bottom-up approach, whereby Organisational Units (OUs') within O/M/As are the initiators. The initiatives from OUs' are usually based on their own sectorial interest, with little or no concern for the needs of other organisations. This situation has led to the formation of information islands and the duplication of system components within the Public Service of Namibia (NPSCOIT, 2004).

In 2004, the Office of the Prime Minister (OPM) conducted an e-Readiness survey within the Public Service in preparation for its e-Governance Policy development initiative. From the survey data gathered, it was established that public service organisations have primarily developed diverse incoherent Information Systems along departmental or functional boundaries with little or no data sharing among Information Systems. These Information Systems were also from a number of different vendors, and mostly incompatible with each other (OPM, 2004).

The findings from the 2004 survey were re-affirmed with the e-Readiness assessment undertaken in 2011 within the Public Service of Namibia. The e-Readiness report (Government of the Republic of Namibia [GRN], 2011) indicates that interoperability between systems were very low and mostly not formal. The e-Readiness report also noted that there have been no initiatives to date on how applications and data between different public service organisations could interact.

The islands of information established and the duplication of infrastructure within the Public Service of Namibia inhibit internal communication and increases service delivery costs. The lack of interoperability furthermore hinders the implementation of the Government ICT policies and the five phases of e-Governance as stated within the National Development Plan Three (NDP 3) (Office of the President [OP], 2008).

The current Public Service of Namibia organisational landscape is complex and compounded with multi-dimensional interoperability problems. To establish interoperability within the current public service organisational landscape poses considerable systemic and technical challenges. It is therefore essential to define a Public Service specific interoperability direction and to develop, standards and guidance for the establishing of interoperability within this context.

1.3 Research Aim

The aim of the research was to create a Public Service centred cooperative architectural model that defines and guides the establishing of technical interoperability within the context of the Public Service of Namibia.

1.4 Research Questions

In accordance with the aim of the research stated previously, the study answered the following questions:

Question 1: *Which forms of technical interoperability exist within the Public Service of Namibia?*

Question 2: *What forms of models will be required to establish technical interoperability within the Public Service of Namibia?*

Question 3: *What factors will influence the adoption of interoperability within the Public Service of Namibia?*

1.5 Significance of the Study

The research contributes towards a critical discussion on the technical interoperability state and the adoption issues within the context of the Public Service of Namibia.

The research additionally defines and proposes suitable theoretical solutions to establish technical interoperability within the Public Service. In particular the research contributes an application domain specific cooperative interoperability architectural reference model that serves as a technical interoperability blueprint for transforming the Public Service of Namibia into a connected entity that responds to the needs of its stakeholders, customers and citizens.

The establishing of interoperability within the Public Service of Namibia will increase access to data and information, promote data and information sharing and cooperation amongst public service organisations, increase efficiency, stimulate innovation, increase access to the public service and reduce service delivery costs.

1.6 Scope of the Study

This study concentrated on the overall technical dimension of interoperability within the Public Service of Namibia, which consists of technical and syntactical aspects of interoperability. The technical and syntactical interoperability study was limited to the technical interoperability areas of data, software, communication and physical interoperability.

The study focused on devising a cooperative technical interoperability architecture model, taking into account the current technical interoperability state, technical interoperability needs and issues of the Public Service of Namibia. Specific technical interoperability issues that may occur were not addressed; these issues can be addressed by using the cooperative technical interoperability architecture model as it provides a holistic approach to deal with technical interoperability aspects.

To establish the principles and requirements for the cooperative technical interoperability architecture model the focus of the study was directed towards studying the current and required state of technical interoperability, and the factors that may influence the adoption of interoperability solutions by the Public Service of Namibia.

1.7 Research Methodology

The study made use of a qualitative research approach in which explorative research was combined with case study research methods for collecting data.

The population sample consisted of Public Service IT Managers and IT Staff who were responsible for operationalized Information Systems. Data was obtained by using both purposive and snowball sampling methods. Both semi-structured interviews and formal structured walkthroughs were used to gather data from the identified population. The semi-structured interview process was guided by an interview guide whereas the structured walkthroughs were guided by a checklist.

The data gathered was summarised, ranked and described using descriptive statistical methods. The processing and analyses of the data gathered was performed using different instruments and statistical software programmes.

1.8 Summary of the Findings

The analysis performed of the data analysis findings indicated that technical interoperability between Information Systems was at a low level of technical sophistication with the majority of Information Systems exchanging data through manual or ad-hoc means. The data analysis findings further indicated that technical interoperability was limited to 15 Information Systems within 11 public service organisations. The level of

technical interoperability sophistication and compliance between interoperability Information Systems was found to be overall at a low level.

From the data analysis findings it was found that there was a need to increase the level of technical interoperability sophistication between Information Systems and to expand the number of technical interoperability Information Systems within the public service. The data analysis findings suggested that a hybrid form of interoperability architectural model was required to increase technical interoperability within the public service. The hybrid architectural model required by the public service should include architectural aspects of the Client-Server, Peer-to-Peer and Service Oriented forms. A suitable cooperative architectural reference model was designed based on the analysis findings.

The analysis further identified a number of interoperability adoption factors that may impact on the establishing of interoperability within the Public Service of Namibia. The interoperability factors of 'Data Security' and 'Data Quality' were the factors most identified by respondents that may influence the adoption of interoperability within the public service.

1.9 Definition of Terms

The following are frequently used terms within this thesis.

Architecture: Representation of the structure of a system that describes the fundamental organisation of its components, their relationships to each other, and to the environment, and the principles that guide its design and evolution.

Component: Independent unit of software that is completely defined and accessed through a set of interfaces.

Data Interoperability: Denotes the ability of heterogeneous systems to understand the syntactical and semantic meaning of data from different data models through the use of common data models, mappings and structures.

Enterprise Architecture: Represents the meta-architecture of an organisation or the overall assembly of all architectures of an organisation.

Heterogeneous: The variety and differences of computer networks, hardware and software.

Interface: Mechanism by which a component describes its functionalities and provides access to its services. Provides attribute specifications and operations associated with software components.

Interoperability: The ability of information technology systems to exchange data and share information and knowledge in uniform and efficient manner. Interoperability includes organisational, data and technical aspects that relate to data exchange and information and knowledge sharing.

Middleware: Infrastructure software within a distributed system that helps to manage interactions between the distributed entities in the system and the databases.

Organisational Interoperability: Focuses on bringing about collaboration of administrations that wish to exchange data but who have different internal structures and procedures.

Peer-to-Peer Architecture: Is an architecture in which each peer has the same capabilities and either peer can access and exchange files with each other directly.

Service: Distinct unit of functionality provided to clients that perform one or more operations and returns a set of results to the requester.

Reference Architecture: A generic system architecture that is an idealised architecture that includes all the features those systems might incorporate.

Service Oriented Architecture (SOA): Architecture in which functionalities are provided by a service that is exposed using the Internet (XML, TCP/IP) as a transport mechanism.

Software Architecture: A model of the organisation and structure of a software system, which comprise software elements and the relationships among them.

Systems Architecture: A formal description of a system, or a detailed plan of the system at component level to guide its implementation.

Semantic Interoperability: Denotes the aspects of interoperability that is concerned with ensuring that the precise meaning of exchange data is understood by the receiving system that was not initially developed for this purpose.

Syntactical Interoperability: Represents the interoperability aspects that are associated with data formats and communication protocol syntax and encoding that would allow two or more systems to communicate and exchange data.

Technical Interoperability: Covers the technical issues of linking computer systems and services which includes aspects such as interfaces, interconnection services, data integration, middleware, data presentation, data exchange and security.

1.10 Outline of the Thesis

The thesis is organised into eight chapters.

Chapter 1 introduces interoperability, statement of the problem, research questions for the study, significance of the study, scope of the study, followed by the summary of the research methodology and the findings.

Chapter 2 addresses the literature review carried out for the purpose of the study.

Chapter 3 discusses the research methodologies used in the study.

Chapter 4 discusses the Government Interoperability Governance Model (GIGM) and Government Interoperability Governance Framework (GIGF) that was used to guide the study.

Chapter 5 presents the analysis of the data collected through the semi-interview process from interviewees.

Chapter 6 discusses the findings of the data analysis in relation to the research questions posed in the thesis.

Chapter 7 presents and discusses the design of the Cooperative Architectural Model (CAM) for the Public Service of Namibia that addresses the research aim.

Chapter 8 presents the conclusion for the study and recommendations for further research.

1.11 Summary

The research findings indicated that the establishing of technical interoperability within the Public Service will allow for the sharing and exchanging of data in an agreed upon and standardised manner between organisations. Chapter 1 introduced interoperability, the

statement of the problem and the research questions for the study. The scope and significance of the study, a brief summary of the methodology used, findings made, and the outline of the thesis were also discussed.

In chapter two, the literature reviewed would be discussed in relation to the current knowledge available that is relevant to the study aim and research questions of this thesis.

2. LITERATURE REVIEW

The literature review presents the current knowledge available that is relevant to the study aim and research questions outlined in chapter one. This chapter firstly introduces the different descriptions of interoperability and then discusses previous research and studies available on interoperability forms, measures, adoption factors and models. The chapter concludes with a review of the Government of Namibia's interoperability directives and a chapter summary.

2.1 Introduction

A collection of primary and secondary literature resources was used to obtain relevant facts and background information on different aspects of interoperability that relates to the study. The collection of literature resources used consists of published scientific papers and journals, government publications and books.

The literature was reviewed under six areas, namely:

(1) Descriptive Forms of Interoperability

(2) Aspects of Technical Interoperability

(3) Interoperability Architectural Forms

(4) Measuring Interoperability Maturity

(5) Interoperability Adoption Factors

(6) Government of Namibia's Interoperability Directives

Summaries and comparisons are provided for each of the above mentioned areas of the literature reviewed in the following corresponding sections.

2.2 Descriptive Forms of Interoperability

A number of reports and technical papers have described interoperability in different ways focusing on different components of interoperability such as operational components and technical components.

According to the IEEE (1990), interoperability is the ability of two or more systems or components to exchange information and to use the information exchanged.

Miller (2000) defines interoperability as an on-going process of ensuring that systems, procedures and cultures of an organisation are managed in such a way as to maximise opportunities for exchange and reuse of information.

The European Commission, IDABC (2004), views interoperability as the ability of ICT systems and the business processes they support to exchange data and share information and knowledge.

According to the Australian Ministry of Finance and Deregulation (2005), interoperability is "...the ability to transfer and use information in a uniform and efficient manner across multiple organisations and information technology systems".

The New Zealand Government perceives interoperability as the ability of Government organisations to share and integrate information and business by using common standards (State Services Commission, 2006).

From these definitions of interoperability, one main common thread is found among them all; it is the ability to exchange data and information among multiple organisations.

2.3 Aspects of Technical Interoperability

Interoperability within the public service will need to be addressed at technical, semantic and organisational level (Sanchez, Janowski, & Estevez, 2008).

Technical interoperability is essential to ensure that communication is established within and among government agencies by linking heterogeneous computer systems and services. This includes aspects such as open interfaces, connectivity, data integration, middleware, data presentation, data exchange, accessibility and security issues (Sanchez et al., 2008).

Pankowska (2008) as well as Ray (2009) felt that technical interoperability requires standards concerning middleware, network protocols and security protocols.

According to Lallana (2008), technical interoperability may be established on different layers such as:

(1) Interconnectivity Layer: Enables communication between systems and includes the standards relating to network and systems development.

(2) Data Integration Layer: Enables exchange of data between different systems and contains the standards for describing data.

(3) Information Access and Presentation Layer: Focuses on the various means of presenting data to users through different access challenges.

(4) Content Management and Meta-data Layer: Refers to standards that are required to retrieve and manage Government information.

For technical interoperability to take place between systems, Lallana (2008) expressed the view that a system should meet at least one of the following requirements:

(1) A system generates data that could be used by another system.

(2) A system processes or consumes data that is generated by another system.

(3) A system relies on another system for the delivery of data.

(4) A system uses software that operates on the same platform as another system.

According to Jolma et el. (2003), there are three computationally different ways to achieve interoperability, namely:

(1) Requesting data or documents from a system;

(2) Exploiting the computational resources of a network node through a published interface; and

(3) Sending executable instructions from one network node to another network node.

Pardo et el. (2008) concluded that the degree to which government has developed interoperability business and technology architectures can be described in terms of the existing services, operational components and networks of organisations and how they are connected to each other through business processes and technologies.

From the literature reviewed, the majority of the authors identified interoperability standards as a key issue to be addressed. In general, authors were in agreement that technical interoperability involves as a minimum hardware, software and data. Different viewpoints were also expressed of what makes systems technical interoperability.

2.4 Distributed Systems Architectural Forms

The main motivation for creating distributed systems is resource sharing among different heterogeneous systems (Coulouris, Dollimore, & Kindberg, 2009). This capability makes this form of architectural form most suitable for establishing interoperability between different types of systems.

Tanenbaum & Van Steen (2007) defined a distributed system as a collection of independent computers that appear as a single coherent system to its users. Coulouris et al.

(2009) viewed a distributed system as a system were the hardware or software components of networked computers communicate and coordinate their actions by passing messages.

According to Coulouris et al. (2009) distributed systems can be described in terms of their software architecture and their system architectures which determine their appearance, structure and style. These two aspects form the concept of an architectural model.

The term software architectures refer to the logical organisation, interaction and structure of software components within a computer (Tanenbaum et al., 2007). System architecture on the other hand looks at the division of system components responsibilities and the placement of these components across networked computers (Coulouris et al., 2009; Tanenbaum et al., 2007). System architectures reflect the final instantiation of software architecture (Tanenbaum et al., 2007).

Tanenbaum et al. (2007) identified four distinct architectural styles for distributed systems such as:

(1) **Layered Architectures:** In this style, components are organised in a layered fashion, where control flows from layer to layer. Requests move down component hierarchy while results flow upwards.

(2) **Object-Based Architectures:** Object-Based Architectures are more loosely organised than layered architectures and are connected through remote procedure call mechanisms.

(3) **Data-Centred Architectures:** This style uses a common passive or active repository that allows processes to communicate.

(4) **Event-Based Architectures:** In Event-Based Architectures processes are loosely coupled and communicate through the propagation of events (e.g., publisher/subscriber systems).

Tanenbaum et al. (2007) classified systems architectures broadly into centralised, decentralised and hybrid architectures. Sommerville (2007) and similarly Tanenbaum et al. (2007) identified a number of common distributed systems architectures that are mostly used by designers, namely:

(1) **Client-Server Architecture (Centralised Architecture):** This architecture is the most common and widely employed distributed architecture. Processes are divided into two groups, the server process and client process. The client processes interact with individual server processes in order to access shared resources managed by servers. Systems of this type can be easily implemented and optimised. However, once the Client-Server system is established it is difficult to change the functionality of the system.

(2) **Peer-to-Peer Architecture (Decentralised Architecture):** In this type of architecture all processes have a similar and equal role, with no distinction between the client and server processes. Processes are organised into an overlay network in which every process has a local list of every peer it can communicate with. Every process that participates in the system provides services to and consumes services from others. This type of architecture is very dynamic, self-organising and flexible since any similar process can join the system at any time and start exchanging data with other processes. Peer-to-Peer systems suffer from reliability and scalability problems.

(3) **Distributed Object Architecture (Hybrid Architecture):** In a distributed object architecture (e.g., CORBA, RMI), the system components are objects that provide interfaces to services that they provide. Objects may call these services with no logical distinction between a receiver and a server of a service. Objects may be distributed across a number of computers across the network. Communication among objects is through the object request broker middleware. This form of architecture is very flexible and the reuse factor is very high.

(4) **Service Oriented Architecture (Hybrid Architecture):** Represents an approach to distributed computing that treats software resources as discoverable resources on the network. All functions are defined and published as independent services. Services define the logical interaction between service providers and service consumers through one or more service interfaces. Service interfaces define the data available and how it can be accessed. Services can be invoked through a service bus in defined sequences to form business processes accessible via an application front-end. The Service Oriented Architecture allows applications to interact with the minimum cost and effort. Services provided through this architecture are reusable, which is its major advantage.

From the literature reviewed, it is evident that a variety of architecture styles and forms are available to model designers that want to develop interoperable solutions to achieve distribution transparency and adaptability within the Public Service. The decision on which architectural style and form to employ will be influenced by an organisation's needs, standards and agreed upon design principles.

2.5 Measuring Interoperability Maturity

Maturity models describe the stages of progress or evolution through which systems, processes or organisations progress (Clark & Jones, 1999).

A variety of interoperability maturity models have been developed, each adopting a unique vocabulary to express their characterisation of interoperability capability maturity. These maturity models address certain specific problem domains.

In 1993 the Levels of Information Systems Interoperability (LISI) project was initiated by the C4ISR Integration Task Force to address the specific requirements of C4I (Command, Control, Computer, Communication and Intelligence) domain. The outcome of the LISI project was a LISI reference model and process for defining, assessing and certifying the degree of interoperability required or achieved between organisations or systems. The LISI Interoperability Maturity Model defines five stages of increasing levels of sophistication regarding system interaction and the ability of the system to exchange and share information and services (C4ISR, 1998). An overview of the LISI Interoperability Maturity Model is depicted in Table 2.1.

Table 2.1: Overview of the LISI Interoperability Model (C4ISR, 1998)

Levels	**Information Exchange**
(5) Enterprise Interactive manipulation; shared data and applications	• Distributed global information and applications • Simultaneous interactions with complex data • Advanced collaboration • Event-triggered global database update
(4) Domain Shared data; separate applications	• Shared databases • Sophisticated collaboration
(3) Functional Minimal common functions; separate data and applications	• Heterogeneous product exchange • Basic collaboration • Group collaboration
(2) Connected Electronic connection; separate data and applications	• Homogeneous product exchange
(1) Isolated Non-connected	• Manual gateway

The Organisational Interoperability Maturity Model for C2 was proposed by Clark and Jones (1999) and serves to compliment the LISI reference model by extending it into the area of organisational interoperability. The Organisational Interoperability Maturity Model for C2 (see Table 2.2) defines five levels of organisational maturity of which each level is defined by one or more primary enabling attributes.

Table 2.2: Summary of Organisational Interoperability Maturity Model for C2 (Clark and Jones, 1999)

Levels	Preparedness	Understanding	Command Style	Ethos
(5) Unified	Complete normal day-to-day	Shared	Homogeneous	Uniform
(4) Combined	Detailed doctrine and experience in using the doctrine	Shared communication and knowledge	One chain of command and interaction with home organisation	Shared ethos but with influence from home organisation
(3) Collaborative	General doctrine in place and some experience	Shared communication and knowledge about specific topics	Separate reporting lines of responsibility overlaid with a single command chain	Shared purpose; goals value system significantly influences home organisation
(2) Ad-hoc	General guidelines	Communication and shared information	Separate reporting lines of responsibility	Shared purpose
(1) Independent	No preparedness	Communication via phone	No interaction	Limited shared purpose

Sarantis, Charalabidis & Psarras (2008) proposed the Government Interoperability Model Matrix (GIMM) that can be used by organisations to assess their current e-Government Interoperability status in respect to interoperability readiness and performance. The GIMM (see Table 2.3) defines five different sets of organisational interoperability maturity levels, where each level corresponds to a different interoperability level for a set of Interoperability Attributes (IA). The organisational interoperability maturity levels defined in GIMM are closely aligned to the LISI reference model and very similar to the Organisational Interoperability Maturity Model for C2 levels.

Table 2.3: Summary of GIMM (Sarantis et al., 2008)

	Type of Organisation				
	Independent	**Ad-hoc**	**Collaborative**	**Integrated**	**Unified**
System	Informational website	Electronic ad-hoc exchange of information with other organisations	Interoperability goals are recognised and, roles and responsibilities are allocated. Distinct organisation.	Organisation has shared value systems and shared goals, common understanding with other organisations and is prepared to interoperate with other organisations.	Organisation is fully interoperable with front and back office systems of other organisations.

The interoperability maturity models reviewed (i.e., LISI, C2 and GIMM) define very similar interoperability maturity levels with the main differences between the models being their focus and the manner in which they rate interoperability. The models reviewed are partial models that deal with some aspects of the enterprise interoperability domain. An interoperability maturity model covering all areas of concern and aspects of enterprise and e-Government interoperability is still missing.

Interoperability maturity models like GIMM provide the basic means to assess an organisation's current interoperability state and services, providing a deeper understanding of its interoperability context. These models further help organisations to take a functional view of their interoperability both at organisational and at an Information System level.

2.6 Interoperability Adoption Factors in the Public Service

The adoption of an interoperability solution will be influenced by a number of factors. The factors that influence the adoption process will differ between different types of organisation, leading to different viewpoints (Kamal, Themistocleous & Elliman, 2008).

Ray (2009) proposed a research framework that would influence the adoption of interoperable technology for Government Information System. Ray (2009) postulated that interoperable technology for Government Information System would be influenced by technology factors, organisational factors and environmental factors (see Table 2.4).

Table 2.4: Interoperability Technology for Government IS Adoption Factors (Ray, 2009)

Characteristic	**Adoption Factors**
(1) Technical Influence of technology innovations on the adoption process.	• Benefits • Barriers • Compatibility • Complexity
(2) Agency Internal characteristics that might impact information sharing.	• IT capability • Top management support • Agency championship • Type of Government
(3) Environmental Characteristics of the environment that might impact on the operations of local agencies.	• External influence • Policy/legal framework • Critical mass

A conceptual model for Government-to-Government (G2G) information sharing in the e-Government environment was proposed by Fan & Zhang (2007). The model is composed of four levels (see Table 2.5), each containing different factors that will motivate organisations to exchange and share information.

Table 2.5: G2G Information Sharing Model (Fan et el., 2007)

Levels	Motivation Factors
(1) Environmental Level Refers to the external support and guarantee for G2G information sharing.	• Legal/Policy framework • Project wide championship
(2) Inter-organisation level Refers to the coordination and issues government agencies have to deal with in the information sharing process.	• Trust across agencies • Social networks • Organisational Compatibility
(3) Intra-organisational Level Refers to the G2G information sharing factors that organisations have to prepare for.	• Top organisation support • Operation cost • Process security • IT capability • Process traceability
(4) Perceived Performance Refers to the benefits and risks of G2G information sharing within the e-Government environment.	• Perceived benefits • Perceived risks

Kamal et al., (2008) proposed an Enterprise Integration Architectural (EIA) adoption model for Local Government Agencies (LGAs). The model groups together different EIA adoption factors (see Table 2.6) that will influence the EIA decision making process within LGAs.

Table 2.6: Factors Influencing EIA adaption within LGAs (Kamal et el., 2006)

Factor Categories	Adoption Factors
(1) Pressure Factors	• Project champion • Citizen's satisfaction • Critical mass • Market knowledge
(2) Technology Factors	• Evaluation frameworks • Technology risks • IT capabilities (IT infrastructure, knowledgeable personnel, IT sophistication) • Data security and privacy
(3) Support Factors	• Top management support • IT support • Higher administration authority
(4) Financial Factors	• Financial capability (Return on investment, cost)
(5) Organisational Factors	• Managerial capability • Barriers • Benefits • Formalisation • Organisational size

From the above factors mentioned, there are several common adoption factor attributes that may influence the adoption of interoperability within an e-Government environment such as: (a) costs, (b) project championship, (c) critical mass, (d) external factors, (e) perceived benefits, (f) perceived risks, (g) IT support and (h) top management support.

Adoption factors can be used as an approach to identify specific elements that will influence the acceptance of an interoperability architecture design by an organisation. The identified adoption factor elements can further serve as a reference that should be taken into account during the interoperability solution design process.

2.7 Government of Namibia Interoperability Directives

The Namibian Government has enacted three policies that provide some interoperability directives and guidelines. The implementations of these policies are provided for in NDP 3 (OP, 2008).

The e-Governance Policy for the Public Service of Namibia of 2005 makes provision for the establishing of an Interoperability Framework Policy that should provide standards and specifications for data integration, interconnectivity and information access. The e-Governance Policy further requires that common standards and infrastructure, as well as a middleware service gateway be established to enable interoperability and joined-up services (OPM, 2005).

The IT Policy for the Republic of Namibia (MICT, 2008) as well as the Overarching ICT Policy for the Republic of Namibia (MICT, 2009) contains policy statements relating to electronic connectivity (e-Connectivity). The provisioning for e-Connectivity in both policies requires that reliable, real-time, secure two-way connectivity be established with constituencies and within Government. These policies also promote the sharing of information and infrastructure among public service organisations, regional and local authorities.

In addition to the above mentioned interoperability policy directives, NDP 3 (OP, 2008) stipulates that Government should implement the five stages of e-Government evolution model as defined in the United Nations e-Government Survey report of 2008 (UNDESA, 2008).

The fifth stage of the e-Government evolution model (Department of Economic and Social Affairs, 2008) relates to interoperability. This stage focuses on the connected Government

that transform themselves into a connected entity by developing and integrating the back office infrastructure. This level is characterized by connections such as:

(1) Horizontal connections (among government agencies);
(2) Vertical connections (central and local government agencies) ;
(3) Infrastructure connections (interoperability issues) ;
(4) Connections between governments and citizens; and
(5) Connections among stakeholders (government, private sector, academic institutions, NGOs and civil society).

The Government interoperability directives set the direction for the type and form of interoperability that needs to be established. These directives will need to be taken into account when developing interoperability frameworks, standards and architectures.

2.8 Summary

The literature review provided deeper insight into the different interoperability descriptions, models, maturity measures, adoption factors and forms of interoperability.

From the literature reviewed, it was gathered that there are a number of different viewpoints and methodologies regarding interoperability maturity, adoption and technical interoperability forms available for use by public services.

The literature reviewed on Government Policy and Development Plans, provided some insight into the Government of Namibia's interoperability direction and requirements.

The literature reviewed on interoperability maturity and adoption was used in the research to formulate the conceptual frameworks for the study whereas the literature reviewed on interoperability forms was used to inform the interoperability architecture development process.

The following chapter explains the research methodology employed for this research.

3. RESEARCH METHODOLOGY

The aim of this chapter is to present the research methodology used in this study. The presentation of the research methodology includes a discussion of the research design, research instruments developed and the model validation approach employed. The chapter concludes with a summary of the chapter.

3.1 Introduction

The research methodology used was directly linked to the research questions of this study. The overall research methodology employed is illustrated in Figure 3.1 and elaborated on further in the next section.

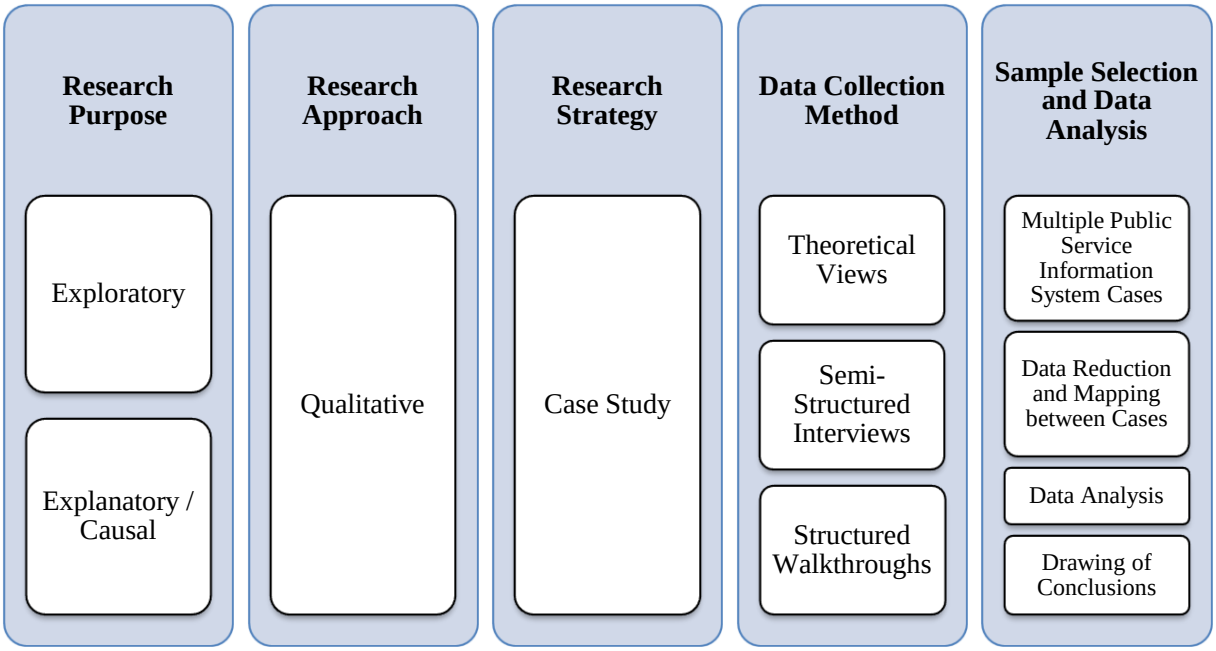

Figure 3.1: Summary of Research Methodology

For the purpose of reference, the study aim and research questions are listed below:

The aim of the research was to develop a public service centred cooperative architectural reference model that defines and guides the establishing of technical interoperability within the context of the Public Service of Namibia.

In accordance with the research aim, the study concentrated on the following research questions:

Question 1: *Which forms of technical interoperability exist within the Public Service of Namibia?*

Question 2: *What forms of models will be required to establish technical interoperability within the Public Service of Namibia?*

Question 3: *What factors will influence the adoption of interoperability within the Public Service of Namibia?*

The outcomes of the research questions provided the inputs for formulating the conceptual interoperability architectural model in-line with the research aim. The inquiry process was concluded when it was successfully demonstrated that the conceptual interoperability architectural reference model agreed with the interoperability needs and architectural principles identified through the research questions.

3.2 Research Design and Methods

The primary focus of the study was to obtain a better understanding of interoperability within the public service and to generate interoperability architectural design knowledge that could be used to inform and guide interoperability Information Systems development processes. To realise the study aim, there was a need to understand the current technical interoperability environment, technical interoperability needs and interoperability adoption factors that may have bearing on the development of an interoperability architectural model for the Public Service of Namibia.

To answer the research questions a qualitative research approach of descriptive type was used in which explorative research was combined with case study research. Qualitative

research was used to investigate technical interoperability within the environment of the Namibia Public Service with the intention to explore different viewpoints and to obtain a deeper understanding of the technical interoperability environment, needs and issues.

The explorative research conducted provided deeper insight into existing theoretical views and explicit knowledge on technical interoperability and its adoption. Explorative research was conducted primarily through literature studies.

The objective of the case study research conducted was to investigate the interoperability dynamics of public service organisations. The cases studied provided a better understanding of the uniqueness and idiosyncrasy of technical interoperability and the factors that may influence technical interoperability adoption in all its complexity. Particular focus was given to identify recurring patterns, differences and irregularities.

Cases were represented by Information Systems that were exchanging data. Data for each of the cases studied was gathered through semi-structured interviews. The multiple cases studied provided an opportunity to compare and contrast different cases. The different interviews conducted for each case providing the means of collaborating responses.

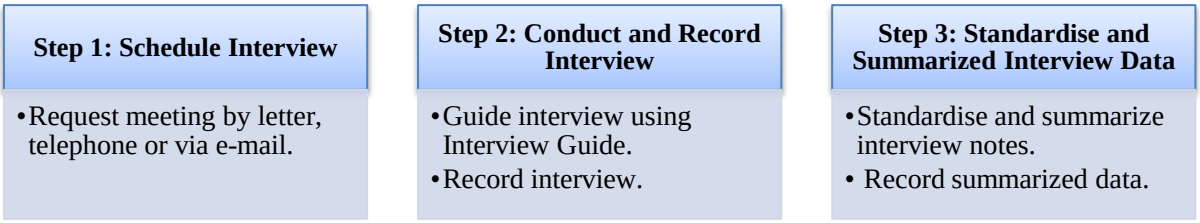

Figure 3.2: Semi structured Interview Process

The semi-structured interview process used, followed a three step process as indicated in Figure 3.2. The semi-structured interview process commenced with the scheduling of the interview and ending with the standardising and summary of the raw interview data collected.

To guide the semi-structured interviews, an interview guide (see Section 3.5.2) was utilised that consisted of themes (topics) and relevant guiding questions. During each interview, interview notes were made for each topic discussed. The interview notes were standardized and documented using an Interview Results Framework Tool (see Section 3.5.3).

The specific research approaches employed to answer the research questions are presented in the following three sections.

3.2.1 Methodology for Answering Research Question One

Semi-structured interviews were conducted to establish the current forms of technical interoperability present within public service. Interview data obtained were standardised and documented. The documented interview results were grouped and combined to form pairs of Information Systems that were exchanging data with.

The different interoperable Information System pairs were tabulated and analysed. As part of the analysis, cross case analysis of the interoperable pairs of Information Systems were performed.

3.2.2 Methodology for Answering Question Two

Question Two was answered by combining existing theoretical views and explicit knowledge with the requirements of the Public Service.

Literature research was conducted to gather and analyse existing theoretical views and explicit knowledge of technical interoperability. Semi-structured interviews were conducted to obtain the technical interoperability requirements of the Public Service.

The data gathered through the semi-structured interview process was standardised, abstracted and recorded on interview results forms. The documented data was combined, analysed and mapped to existing theoretical views. From the data analysis and data

mappings the final conclusions were drawn that led to the formulation of the technical interoperability architecture model.

3.2.3 Methodology for Answering Research Question Three

Semi-structured interviews were conducted to establish the factors that may influence the adoption of interoperability by the public service.

Data was gathered through semi-structured interviews through the semi-structure interview process as illustrated in Figure 3.2. The data gathered was standardized, abstracted and recorded on interview results forms. The different abstracted interview results were combined, tabulated and analysed. Statistical analysis was performed using the MoonStats 2 and Microsoft Excel 2010 application software.

3.2.4 Methodology Used to Validate Theoretical Architectural Models

The goal of the validation process is to make certain that models developed address the objectives and provide accurate information about the domain being modelled (Satzinger, Jackson, & Burd, 2002). Validation ensures that the models conform to their specifications and meet the expectations of the customers, establishing credibility in the model (Sommerville, 2007).

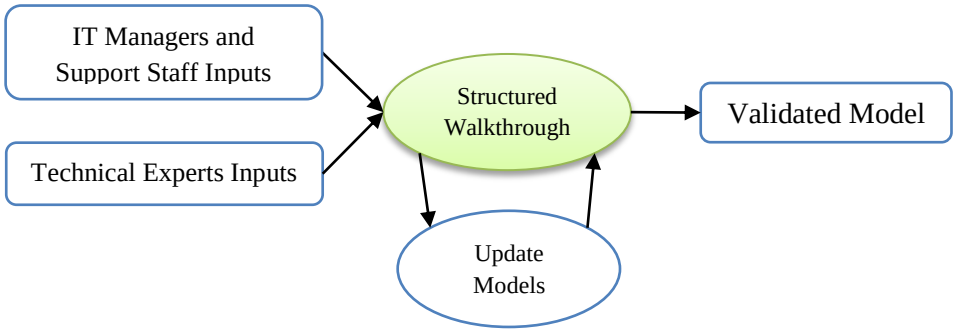

Figure 3.3: Structured Walkthrough Process

The cooperative architectural model was validated by an expert group through a formal structured walkthrough process (see Figure 3.3) as described by the U.S. Department of Energy (2002). Formal structured walkthroughs is a powerful review technique that can be used to validate designs and verify internal consistencies (Satzinger et el., 2002).

Structured walkthrough was conducted with a selected group of IT Managers, operational staff and technical experts. To guide the structured walkthrough process a checklist was utilised. All issues identified during the structured walkthrough process were recorded on a control sheet (see Appendix E). Where applicable, the feedback received was applied to the conceptual cooperative interoperability model.

The conceptual cooperative interoperability architectural model was deemed validated and complete with the sign-off of the model by the selected group of experts. With the sign-off of the conceptual cooperative interoperability model, the purpose of the research was achieved.

3.3 Population

The target population of analysis consisted of Public Service IT Managers and IT Staff that are directly responsible for operational interoperable Information Systems within the Public Service of Namibia.

3.4 Population Sample

Non-probability type sampling was used to sample members of the population. Individuals who possessed the knowledge and experience relating to the research were sampled by means of purposive and snowball sampling from the various public service organisations.

The purposive sampling method was used to identify IT Managers that were responsible for interoperable Information Systems, whereas snowball sampling was used to identify additional IT support staff within each of the public service organisations.

Through the sampling process, viewpoints were gathered from twenty-six staff members of whom seven were IT Managers and 19 IT support staff. These staff members were responsible for 15 interoperable Information Systems. From these Information Systems, 12 unique pairs of Information Systems were exchanging data.

3.5 Design of Research Instruments

To conduct the study, a number of research instruments were designed using the knowledge gathered through the literature reviewed. The most important instruments designed and utilised during the study are described in the following sections.

3.5.1 Study Reference Framework

To guide the study of the different interoperability forms and interoperability adoption factors, a broad Government Interoperability Governance Model (GIGM) and associated Government Interoperability Governance Framework (GIGF) were developed.

The GIGM specifies an overarching interoperability governance model whereas the GIGF serves as an interoperability reference framework aimed at demarcating and guiding the overall process of establishing interoperability within Government.

For the purpose of the study, the data and technical interoperability related aspects (i.e., Collaboration, Standards, Data and Information, and Architecture) of the GIGF were used as technical interoperability frame of reference for developing the different research instruments for the study. These technical aspects of interoperability were studied in terms of the current state of interoperability, perceived future state of interoperability and the

factors that may influence interoperability. Both the GIGM and GIGF are described in more detail in chapter four.

3.5.2 Interview Guide Tool (IGT)

The semi-structured interviews conducted used a fairly open framework that allowed for focused, conversational, two-way communication. A pre-prepared Interview Guide Tool (IGT) based on the GIGF domains of (a) Collaboration, (b) Standards, (c) Data and Information, and (d) Infrastructure (see Section 3.5.1) was designed to guide the semi-structured interviews.

The IGT served the purpose of obtaining qualitative data from the population sample in respect of the following study areas:

(1) Current forms of technical interoperability of the Public Service of Namibia;

(2) Required forms of technical interoperability of the Public Service of Namibia; and

(3) Factors that influences interoperability adoption by the Public Service of Namibia.

Table 3.1: Summary of the Interview Guide Tool (IGT)

Sections	Interoperability Domains	Description
Section 1: General	Collaboration	Questions focused to establish if a public service organization has operational Information System in place and the degree of collaboration between these Information Systems.
Section 2: Current State of Interoperability	• Standards • Data and Information • Infrastructure	Questions focused to determine the forms of technical interoperability used, data shared and the guiding standards in place.
Section 3: Required State of Interoperability	• Standards • Data and Information • Infrastructure	Questions focused to determine the standards, forms of technical interoperability and data required in the future by public service organisations based on their interoperability needs.
Section 4: Interoperability Adoption	• Standards • Data and Information • Infrastructure	Questions directed to establish the different factors that influence the adoption of interoperability by a public service organization.

The four sections as indicated in Table 3.1 of the IGT provided the framework to guide the data collection process. The interview guide that was formulated from the IGT is presented in Appendix A.

3.5.3 Interview Results Framework Tool (IRFT)

To record the results obtained from the interviews conducted, an Interview Result Framework Tool (IRFT) was derived from the domains of GIGF (see Section 4.3). The IRFT (see Table 3.2) provides the means of standardising and summarising interview data obtained for the current and required state of technical interoperability as well as the factors that may impact on interoperability adoption by the public service.

Table 3.2: Interview Results Framework Tool (IRFT)

Domains	**Sub-Domains**	**Attributes**		**Adoption Factors**
		Current State	**Required State**	
Collaboration	Organisations/Entities	Codes (Frequency)	Codes (Frequency)	Keywords (Frequency)
	Information Systems			
	Transfer Mode			
Standards	Interoperability			
Data and Information	Shared Data			
	Data Presentation Format			
	Meta-Content (Data about data contents)			
	Common Data Model			
	Security (Ownership, Rights and Auditing)			
Infrastructure	N-Tier Interoperability Architecture			
	Electronic Services			
	Communication Protocols			
	Communication Network			

The IRFT consists of four domains (see Table 3.2) that correspond to GIGF (see Figure 4.2) inner triangle of four domains. Interview results were coded and identified keyword frequencies calculated for the current and required state of technical interoperability. This process also included the identifying of interoperability adoption factor keywords and keyword frequencies. Standardization was achieved by coding all interview results using the coding schemes defined in Appendix B.

3.5.4 Information System Interoperability Maturity Model (ISIMM)

To assess the degree of interoperability between Information Systems, a practical Information Systems' Interoperability Maturity Model (ISIMM) was devised.

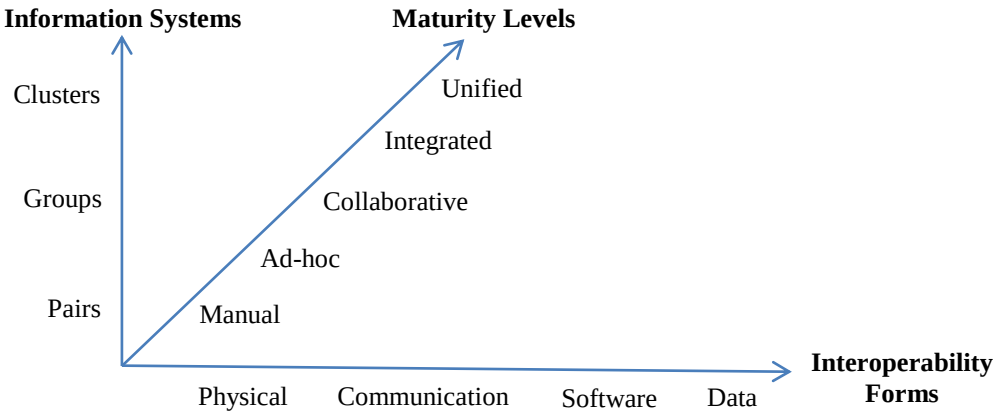

Figure 3.4: Information System Interoperability Model (ISIMM)

ISIMM (see Figure 3.4) defines the levels and degree of interoperability sophistication that an organisation's Information Systems will progress through. The levels of ISIMM provide a structured and systematic approach for assessing and measuring Information Systems' interoperability maturity. In addition to exploring the complexities of interoperability, ISIMM provides the means to attain a deeper understanding of Information Systems' interoperability that will help to promote and establish an interoperable systems environment.

The interoperability levels used in ISIMM are from the Interoperability Coalition Model of section 4.3 whereas the interoperability compliance attributes were derived from the GIGF facets (see Section 4.3.2). The ISIMM maturity levels were derived from the maturity levels of the LISI (C4ISR, 1998) and GIMM (Sarantis et al., 2008) models.

3.5.4.1 ISIMM Maturity Levels

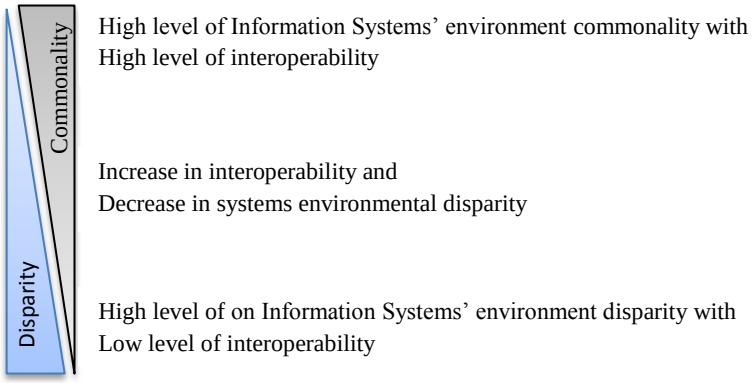

Figure 3.5: Information Systems' Interoperability Maturity Transition

The interoperability maturity levels of ISIMM as depicted in (see Figure 3.5) define the progression of an interoperable environment from a high disparate Information Systems' environment to a high common integrated and shared Information Systems' environment. This categorises a move from a low level to a high level of Information Systems' environment interoperability.

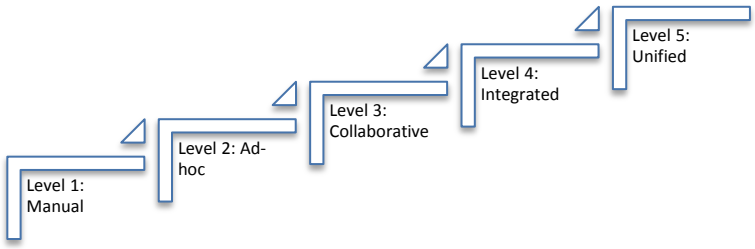

Figure 3.6: Information Systems' Interoperability Maturity Levels

The following maturity interoperability computing environment levels (see Figure 3.6) are contained within ISIMM (see Figure 3.4) such as:

Level 1 – Manual: Information Systems are not connected and data sharing between systems are through manual means.

Level 2 – Ad-Hoc: Basic data sharing of non-standardised data take place through simple electronic means with other organisations. Applications and databases are separated and

data is not shared between organisations. Data are exchanged between systems in a point-to-point manner on an ad-hoc basis.

Level 3 – Collaborative: At this level a wider connection to legacy systems are facilitated. Basic collaboration takes place at a program level between independent applications in a distributed manner. Logical data models are shared and used in the data exchange process. Minimal common functions exist, applications and databases are separated and data is not shared.

Level 4 – Integrated: Data in the integrated stage are shared to some degree and data is exchanged between independent applications using shared domain based data models. Collaboration is at an advanced domain level. Integration of services or systems is being implemented between organisations.

Level 5 - Unified: In the unified stage, data and applications are fully shared and distributed between organisations. Collaboration is at an advanced enterprise level with organisations interoperating on continuous basis through high quality services. Data have a common interpretation and are based on a common exchange model. Front and back office systems are fully interoperable. Processes are also automated at this level.

3.5.4.2 ISIMM Compliancy Levels

ISIMM is visualized in the Information Systems' Interoperability Maturity and Functional Compliancy Matrix in Table 3.3. The compliancy attributes shown in Table 3.3 where abstracted from the literature reviewed on maturity models (see Section 2.5).

Table 3.3: Information Systems' Interoperability Maturity and Functional Compliancy Matrix

Code	Interoperability Layers and Attributes	Levels/Degrees of Interoperability				
		1:Manual (1-4) (2)	**2:Ad-hoc** (5-7) (6)	**3:Collaborative** (8-10) (9)	**4:Integrated** (11-13) (12)	**5:Unified** (14>) (15)
D	**Data Interoperability**	**1**	**2**	**4**	**5**	**5**
1	Common Data Presentation Format	E	E	E	E	E
2	Shared Meta-Content (Data about data contents)			E	E	E
3	Common Data Model			E	E	E
4	Data Security: Ownership, Rights and Auditing		E	E	E	E
5	Shared Data				E	E
S	**Software Interoperability**	**1**	**2**	**3**	**5**	**8**
1	N-Tier Common Interoperability Architecture				E	E
2	Data Exchange Services	E	E	E	E	E
3	Directory Services				E	E
4	Common Naming Services					E
5	Discovery Services			E	E	E
6	Common Workflow Services					E
7	Security Management Services		E	E	E	E
8	Shared Applications					E
C	**Communication Interoperability**	**0**	**1**	**1**	**1**	**1**
1	Common Communication Protocols		E	E	E	E
P	**Physical Interoperability**	**0**	**1**	**1**	**1**	**1**
1	Shared Communication Network		E	E	E	E

The Information Systems' interoperability maturity levels is categorised in the matrix within four dimensions, each consisting of a vector of attributes. Each of these dimensions corresponds to the interoperability layers of: (1) Data Interoperability, (2) Software

Interoperability, (3) Communication Interoperability and (4) Physical Interoperability as described in Section 4.3.

The baseline interoperability functional compliance requirements for each attribute of each interoperability layer are indicated in Table 3.3 with an 'E' (i.e., Expected).

Table 3.4: Information Systems' Interoperability Maturity Ratings Matrix

Code	Interoperability Layers and Attributes	Levels/Degrees of Interoperability				
		1:Manual (1-4) (2)	**2:Ad-hoc (5-7) (6)**	**3:Collaborative (8-10) (9)**	**4:Integrated (11-13) (12)**	**5:Unified (14>) (15)**
D	Data Interoperability	**1**	**2**	**4**	**5**	**5**
S	Software Interoperability	**1**	**2**	**3**	**5**	**8**
C	Communication Interoperability	**0**	**1**	**1**	**1**	**1**
P	Physical Interoperability	**0**	**1**	**1**	**1**	**1**

The range scores for each maturity level/degree are indicated in Table 3.4 at the top of the table (e.g., 1-4, 5-7, 8-10, 11-13 and 14>). The expected level/degree of compliance for each interoperability layer (i.e., D, S, C, and P) is summed in Table 3.4 for each layer and the overall scores are indicated below the range scores at the top of the table. These scores were derived from Table 3.3 for the compliancy attributes marked for each interoperability layer.

3.5.4.3 ISIMM Measurements

ISIMM provides a model to measure the maturity level of interoperability Information Systems for cases such as:

(1) Interoperability maturity and compliance of a specific Information System environment; and

(2) Interoperability maturity and compliancy between pairs, groups or clusters of Information Systems.

Table 3.5: ISIMM Interoperability Measures

Metric Type	Measures	Code
Compliancy	Below the expected level	B
	Expected level	E
	Above the expected level	A
Computing Environment Maturity Levels	Unified	5
	Integrated	4
	Collaborative	3
	Ad-hoc	2
	Manual	1
Interoperability Layers	Data	D
	Software	S
	Communication	C
	Physical	P
Interoperability Attributes	Sub Levels defined from '1' to '8'	1-8

The Information Systems' Interoperability Maturity and Functional Compliancy Matrix (see Table 3.4) and Information Systems' Interoperability Maturity Ratings Matrix (see Table 3.5) services as the instrument to assess both the compliancy as well as the degree of interoperability of an Information System or between Information Systems. A maturity rating is found by identifying the number of compliant attributes for an Information System or pair of Information Systems and comparing the number found with the rating ranges indicated in Table 3.5. The maturity layers defined (see Section 3.5.4.1) should serve as additional guidance in establishing the level of maturity attained.

A scorecard is presented in Table 3.6 to record the level and form of Information Systems' interoperability compliancy between Information Systems.

Table 3.6: Information Systems' Interoperability Scorecard

Information Systems	**System 1**	**System 2**	**System 3**	**System N**
System 1	e.g., 1A			
System 2				
System 3				
System N				

The scorecard (see Table 3.6) is a matrix that consists of Information Systems represented in both the rows and columns. Each row and column intersection indicates the system-to-system interoperability as pairs of values from the interoperability metrics defined in Table 3.5.

Using the compliancy matrix and scorecard different interoperability Information Systems' related views can be compared and studied.

3.5.5 Testing of the Research Instruments

The instruments developed were pre-tested for feasibility, applicability and practicality prior to conducting actual interviews. Pre-testing also served the purpose to correct any shortcomings. The testing of the instruments developed was done through face validity and a pilot study.

Face validity was initially used to validate if the instruments where going to measure what they were supposed to measure. The instruments were face validated by IT experts in the Office of the Prime Minister and computer science lecturers at the University of Namibia (UNAM).

The pilot study was conducted with a selected sample of four that was run through the interview process and results recording process using the IGT and the IRFT. The testing process provided the means of testing and adjusting the IGT, IRFT and ISIMM tools.

3.6 Summary

This chapter addressed the research design, population, sample and research instruments used to study the research questions.

The research design described the qualitative research approach that was followed to answer the research questions. The qualitative research conducted used both explorative and case study methods to gather data from the population.

The population sample consisted of IT managers and staff that were responsible for interoperable Information Systems. The population sample was obtained using both purposive and snowball sampling methods.

A number of research instruments were developed to guide and assist in processing of the data gathered. The research instruments included a study reference framework, interview guide and interview results framework, and interoperability maturity model.

The following chapter will discuss data analysis conducted in relation to the research questions and present the findings of the analysis process.

4. GOVERNMENT INTEROPERABILITY GOVERNANCE MODEL (GIGM) AND FRAMEWORK (GIGF)

This chapter describes the Government Interoperability Model and Framework that were developed to serve as a framework and guide for the study. Attention is also given in this chapter to the relationship between the model and the framework. The chapter concludes with a process cycle for the framework and a chapter summary.

4.1 Introduction

Interoperability is a fundamental building block and enabler of innovative solutions that is required to achieve government's e-Government vision.

On the road to achieving the vision of interoperability, Governments will face many challenges in sharing data and information among autonomous government organisations. A well-developed Government Interoperability Framework (GIF) can help in overcoming most of these challenges and assist governments in effectively implementing e-Government Interoperability across organisational boundaries (Lallana, 2008).

In view of this, the Government Governance Interoperability Model (GIGM) and Government Interoperability Governance Framework (GIGF) were devised to guide the overall development of Government Interoperability in a governed and organised manner. Particular attention is given in addressing the governance concerns of policy, people, procedures and technology in respect of interoperability.

The following sections focus on describing GIGM and GIGF, their relationships and the manner to establish an interoperable organisation.

4.2 Government Interoperability Governance Model (GIGM)

The Government Interoperability Model (GIGM) as depicted in Figure 4.1 is a practical focussed model that defines the areas of activities and their relationships to establish interoperability within a Government. The GIGM is composed of three interdependent areas namely: (1) Strategy and Management, (2) Relationships and (3) Technical infrastructure. By addressing the GIGM focus areas and their inter-relationships a Government will move towards government integration.

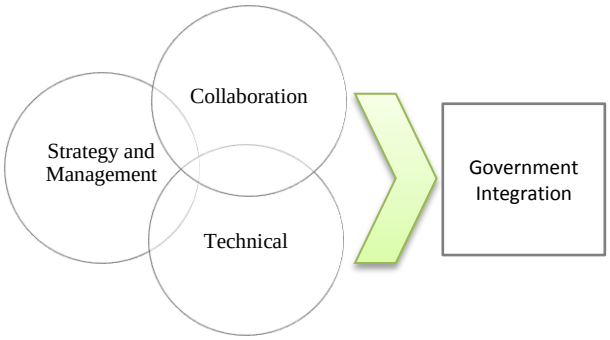

Figure 4.1: Government Interoperability Governance Model (GIGM)

The three areas of the GIGM as depicted in Figure 4.1 are summarised below:

(1) Strategy and Management: The Strategy and Management area of the model refers to the government policy/legal, vision/mission as well as management aspects required to achieve the required state of interoperability. The successful implementation of interoperability related policy and all of its objectives would require a suitable government governance regime. In this sense, interoperability planning and organising within the government is essential to reach alignment with the strategies of government. Strategies and plans developed within this area will impact interoperability both within and across government agencies.

(2) Collaboration: This area focuses on the forms and nature of government collaboration required to meet the overall government strategy. The implementation of a government interoperability solution on top of the existing structures, processes and procedures is

unlikely to add real value to governments. Therefore, government agencies need to evaluate and re-align or redefine their internal processes, procedures and structures.

(3) **Technical:** Technical area of the model that addresses the data and technical standards/architectural issues involved in sharing and exchanging data and information between computer systems. Key elements include standards on areas such as data semantics and syntactic as well as the supporting infrastructure technologies.

4.3 Government Interoperability Governance Framework (GIGF)

The Government Interoperability Governance Framework (GIGF) extends the GIGM to a level of a reference framework. The objective of Government Interoperability Governance Framework (GIGF) is to serve as a common frame of reference that will guide the process of establishing interoperability within a government. The GIGF is focused on establishing interoperability within the six interoperability layers of the Interoperability Coalition Model depicted in Figure 4.2.

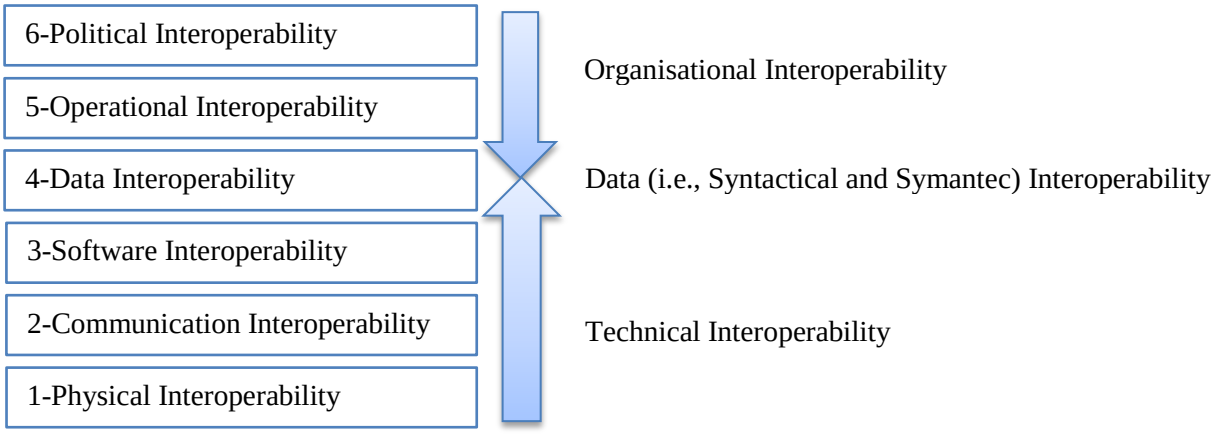

Figure 4.2: Interoperability Coalition Model

The Interoperability Coalition Model as illustrated in Figure 4.2 identifies and demarcates the different interoperability layers in a rank ordered stack. The different layers of the Interoperability Coalition Model are follows:

(6) Political Interoperability: Political interoperability is associated with the guidance and activities of organisations which is ensured by legislation and policy.

(5) Operational Interoperability: Denotes the agreements between organisations and the ability of an organisation to provide services to other organisations through the use of IT (e.g., Information Systems).

(4) Data Interoperability: Data interoperability denotes the ability of different software from heterogeneous systems to understand the syntactical and semantic meaning of data from different data models through the use of common data models, mappings and structures.

(3) Software Interoperability: Refers to the ability of different software used by organisations to work together in exchanging and sharing of data by solving the differences between them.

(2) Communication Interoperability: Communication interoperability denotes the ability of systems to connect and communicate through common protocols.

(1) Physical Interoperability: Physical interoperability is the ability of different computer hardware, network devices and peripherals to work in a connected way.

The GIGF consists of seven connected domains as depicted in Figure 4.3. The GIGF domains as indicated in in Figure 4.3 are grouped into an inner triangle as well as an outer triangle that form the solution framework.

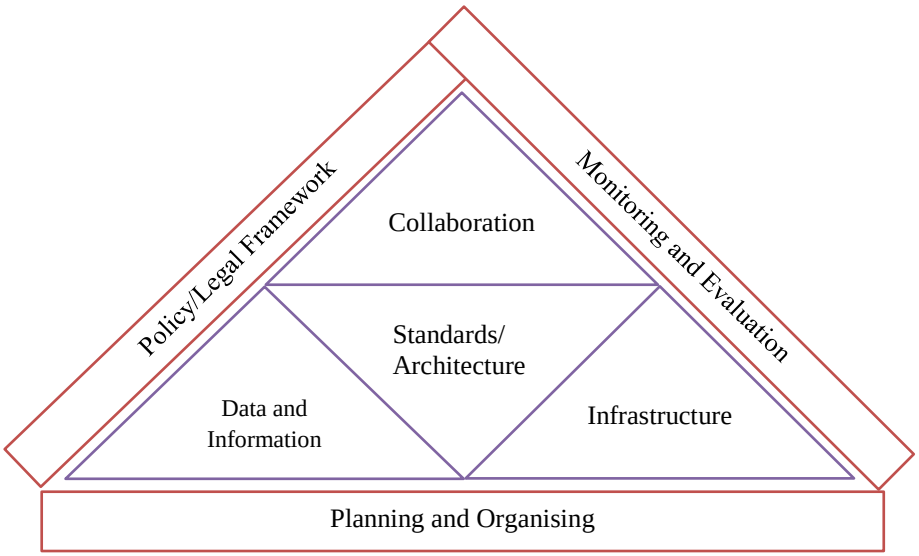

Figure 4.3: Interoperability Governance Framework (GIGF)

The inner triangle of the GIGF (see Figure 4.3) addresses the technical and standards issues of collaborations involved in the exchange and sharing of data and information. The outer triangle of the GIGF (see Figure 4.3) focuses on the organisational aspects of establishing interoperability. The outer triangle drives the development of the facets of the inner triangle of the GIGF.

4.3.1 Relationship of GIGM and GIGF

The GIGM serves as the overarching interoperability governance model whereas the GIGF serves as an interoperability reference framework aimed at ensuring mutual governance and interactions at different levels of interoperability within a government.

The GIGF as depicted (see Figure 4.3) consists of seven interlinked domains which are aligned with the GIGM (see Figure 4.1) areas. The seven domains of the GIGF directly relate to the three areas of the GIGM as indicated in the GIGM-to-GIGF mappings table (see Table 4.1).

Table 4.1: GIGM to GIGF Mapping

GIGM Areas	GIGF Domains
Strategy and Management	Policy/Legal Framework
	Planning and Organising
	Monitoring and Evaluation
Relationships	Collaboration
Technical	Data and Information
	Standards/Architecture
	Infrastructure

Each of the domains of the GIGF expands the higher level GIGM areas into more fine grained detailed reference subsets.

4.3.2 The Domains of the GIGF

The GIGF domains group together governance, organisational and technical issues into seven reference domains. Each domain contains facets of concern that needs to be addressed in order to reach a state of organisational interoperability unification.

Table 4.2: Summary of GIGF Domains and Facets

	Domains						
	Policy/ Legal Framework	**Planning & Organising**	**Monitoring & Evaluation**	**Collaboration**	**Standards / Architecture**	**Data and Information**	**Infrastructure**
Facets (Sub-Domains)	Laws and Policies.	Vision, Objectives/Goals, Overarching Plans, Action Plans, Implementation and Training Structures.	Performance Measures and Tools.	Relationships, Agreements, Trust and Confidence, and Alignment of Processes.	Principles, Standards and/or Conceptual Reference Architecture(s).	Structures, Presentation, Security Classification, Common Data Elements, Ownership, Authentication, Authorization and Auditing.	Communication Infrastructure, Security, Protocols, Open Interfaces, Data Exchange Services, Directories, Naming, Discovery, Common Functions and Access Channels, Technologies.

The seven domains of the GIGF are summarized in Table 4.2. Table 4.2 indicates the minimum organisational, data and technical interoperability related facets of GIGF that an organisation should strive to comply with.

The domains of GIGF are described below:

(1) **Policy/Legal Framework:** The Policy and Legal Framework domain refers to the regulatory and policy frameworks which define the interoperability scale, content, standards and performance references. The development and enactment of policies and/or laws that provide the basis for Government Interoperability should be the first priority.

(2) **Planning and Organising:** Once the policy/legal framework is enacted, plans need to be developed to implement the interoperability directives. Plans should focus on the methodologies and process of establishing interoperability standards/architectures, interoperability infrastructure, data and information.

(3) **Monitoring and Evaluation:** The monitoring and evaluation of interoperability planned activities will play an important role in making certain that targets are met on time and within budget, identified issues are addressed and that compliancy requirements are enforced. To access and measure impact and performance on planned activities, key performance indicators (KPIs), monitoring and evaluation tools and mechanisms needs to be developed.

(4) **Collaboration Domain:** This domain refers to both the nature and level of collaboration within and among government agencies in respect of data and information exchange and sharing. Attention should be given to identifying the different bilateral agreements and process domains involved, level of interoperability (e.g., manual, peer-to-peer, distributed, integrated, global) required, security considerations and compatibility requirements for exchanging data and sharing data and information among organisations. Once this is done, attention should be given to forming of relationships, establishing trust and obtaining top management support for those organisations involved.

To facilitate the synthesis of business processes across the government focus will need to be given to issues concerning the coordination and alignment of business process and architectures of organisations within and outside of government agency boundaries.

(5) Standards/Architecture Domain: The technical aspects of interoperability should be guided by reference or compatibility standards or by conceptual reference architecture. In developing standards/architecture consideration should be given to standards concerning the syntactical and semantics of data to be exchanged and the provision of technology guidance. De facto standards (e.g., XML, Unicode, LDAP) should be adopted as far as possible. The standards selected should be guided by principles such as: scalability, security and privacy and industry support.

(6) Data and Information Domain: Focus in this domain is in describing and developing the data and information structures to exchange and share data and information among computer systems. An important aspect relating to data and information that needs to be addressed is the manner in which data and information will be presented (e.g., documents, objects, graphics and formal messages), shared and accessed by 3rd parties. Attention should also be given to the security classification of data, security access methods and security rights requirements.

(7) Infrastructure Domain: This domain serves the purpose to establish the technical interoperability environment connecting computer systems. Issues of technologies (e.g., hardware, software), communication infrastructure, protocols, open interfaces, electronic services, directories, software architecture (style and topology), security and system management need to be addressed within this domain. The infrastructure will provide the platform and mechanism to exchange and share data and information.

4.3.3 Implementation Process Cycle

To achieve the required level of interoperability among government agencies using the GIGF, issues should first be addressed in the outer layer of the GIGF (see Figure 4.1) triangle moving towards the inner triangle of the GIGF. In a more formal manner, the GIGF may be implemented through seven steps that directly relate to the seven domains of the GIGF as depicted in Figure 4.4.

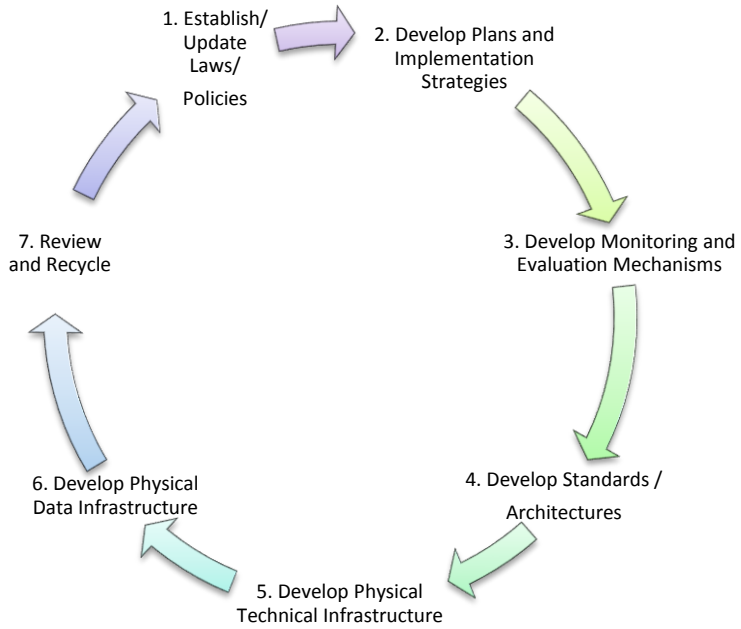

Figure 4.4: GIGF Implementation Process Cycle

The seven implementation steps of the GIGF forms a process cycle (see Figure 4.4) that will be re-iterated for every defined interoperability maturity step that government wants to undertake. The progress made in stepping through the process cycle needs to be monitored constantly and evaluated based on the key performance indicators defined in step three. Feedback and review of the interoperability development progress and issues identified will be performed in step seven of the GIGF process cycle. The learning's obtained from step seven needs to be recycled back into the GIGF process cycle so as to better the interoperability solution quality.

4.3.4 Review of Theoretical Models

The content of this chapter was abstracted and submitted as a conference paper to the 15th World Multiconference on Systemics, Cybernetics and Informatics (WMSCI 2011), Orlando, USA, entitled "Interoperability Governance Model (IGM): Envisages Areas of Activities and Relationships to Establish Information Interoperability within the Government". The paper was peer reviewed and accepted as a conference paper by the WMSCI organising committee. Overall the paper received a rating of 6.7 from the reviewers.

4.3.5 Summary

The GIGM and GIGF provide a holistic approach to establish interoperability on various levels of interoperability. The GIGM provides the overall Government Interoperability Governance Model whereas the GIGF provides the extended reference framework aimed at ensuring mutual governance and interactions at different levels of interoperability within the government.

The GIGF is applied through the GIGF process cycle. The GIGF process cycle may be re-iterated as Government Interoperability matures from a manual to fully unified level of interoperability maturity.

The use of the GIGF will lead to a deeper understanding of Government Interoperability needs and issues and provide the guidance required to establish interoperability at different levels of interoperability maturity. The GIGF will also help decision makers to better focus, plan and manage their interoperability activities, leading to a more efficient and coherent interoperability environment.

5. DATA ANALYSIS FINDINGS

Focus in this chapter is on the analysis of the data gathered through the semi-structured interview process. Analysis of the data is presented within three sections which relate to the research questions. The chapter concludes with a brief summary of the chapter.

5.1 Introduction

In this chapter the analysis of the data gathered through semi-structured interviews and literature studied will be presented in three sections as illustrated in Figure 5.1.

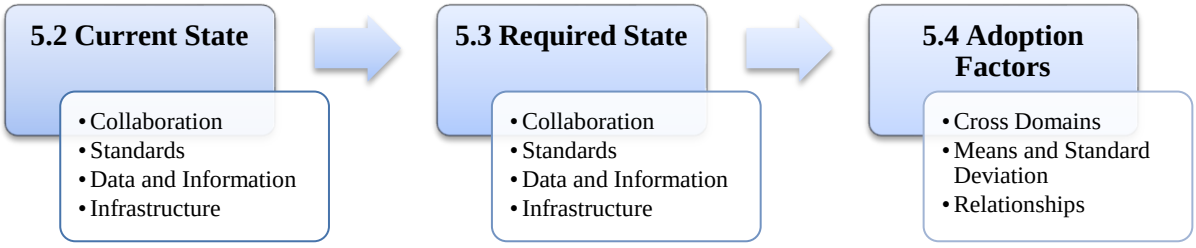

Figure 5.1: Data Analysis and Discussion Outline

A quantitative analysis of the qualitative data collected was performed for the different Information System interoperability cases studied. The combined and summarized data that forms the basis for the data analysis is located in Appendix C and the codes used in the text are located in Appendix B of this thesis.

5.2 Current State of Technical Interoperability

The data gathered was analysed based on the interviewees' perceptions of their current technical interoperability status within different Information Systems' interoperability environments. The summarised data utilised is located in section C.1of Appendix C.

5.2.1 Collaboration

The analyses of the data gathered from the semi-structured interviews are presented in this section for the organisations and Information Systems that were collaborating. The analysis

includes an interoperability maturity assessment of Information Systems that are exchanging data.

5.2.1.1 Organisations Collaborating

The combined organisational collaboration data of the interoperable Public Service organisations are presented in Table 5.1.

Table 5.1: Matrix of Collaborations between Organisations

Organisations	**MFMR**	**MHAI**	**MOF**	**MOLSW**	**MOVA**	**MWT**	**OPM**	**Totals**
MFMR	X							**1**
MHAI		X						**1**
MOF			X	X	X	X	X	**5**
MOLSW			X					**1**
MOVA			X					**1**
MWT			X					**1**
OPM			X					**1**
Totals:	**1**	**1**	**5**	**1**	**1**	**1**	**1**	**11**

From Table 5.1, each row/column intersection marked with an ‘X’ denotes a pair of organisations that are exchanging data. Intra-organisational interoperability is indicated with row/column intersection with the same organisation (e.g., MFMR-with-MFMR). Inter-organizational interoperability is indicated as intersections with different organisations (e.g., MOVA-with-MOF).

Table 5.2: Summary of Organisations Collaborating

No.	Organisations	Collaboration Sectors		
		Internal	**Public Service**	**Total**
1	Ministry of Finance (MOF)	1	4	5
2	Ministry of Fisheries and Marine Resources (MFMR)	1	0	1
3	Ministry of Home Affairs and Immigration (MHAI)	1	0	1
4	Ministry of Labour and Social Welfare (MOLSW)	0	1	1
5	Ministry of Veterans Affairs (MOVA)	0	1	1
6	Ministry of Works and Transport (MWT)	0	1	1
7	Office of the Prime Minister (OPM)	0	1	1
Totals:		**3**	**8**	**11**
Average:		**0.43 (27%)**	**1.14 (73%)**	**1.57**

Table 5.2 illustrates the degree to which Public Service organisations have formed collaborations to exchange data. Analysis of Table 5.2 indicates that seven organisations were exchanging data, with the 'Ministry of Finance' (5) having the largest number of data exchange partners. The rest of the organisations were exchanging data with the same number of organisations (1). On average it was found that every organisation was exchanging data with at least one other organisation.

The data from Table 5.2 further indicates that most organisations have established data exchange collaborations with other public service organisations (73%) followed by internal organizational data exchange partnerships (27%). This indicates that inter-organizational data exchanges are still very limited (27%).

5.2.1.2 Interoperable Information Systems

Data from the interview results was analysed based on the Information Systems that were technical interoperable within the Public Service. From Appendix C, 12 unique

Information Systems pairs were found to be exchanging data. The summarized data for the 12 unique Information Systems pairs are presented in Table 5.3.

Table 5.3: Summary of Information Systems Data Exchange Partnerships

No.	Information Systems	Partnerships
1	Integration Financial Management System (IFMS)	7
2	Fisheries Information Management System (FIMS)	3
3	Government Payroll System (GPS)	2
4	Automated System for Customs Data and Administration (ASYCUDA)	1
5	Daily Subsistence Allowance System (DSA)	1
6	Economic Database (ECO)	1
7	Government Garage Fleet Management System (GGFS)	1
8	Human Resource Information Management System (HRIMS)	1
9	Inland Revenue System (IRS)	1
10	Marine Survey System (MSS)	1
11	National Passport System (NPAS)	1
12	National Population Registration System (NPRS)	1
13	Research Database (RESDAT)	1
14	Social Welfare System (SWS)	1
15	Veterans' System (VETS)	1
Totals:		**24**
Average:		**1.6**

The Information Systems with their number of technical interoperable partners are summarized and ranked in Table 5.3. Table 5.3 shows that 24 partnership combinations were established among 15 different Information Systems. From the 15 Information Systems exchanging data, the 'Integration Financial Management System' (7) was technical interoperable with the largest number of Information Systems followed by the 'Fisheries Information Management System' (3) and 'Government Payroll System' (2). The rest of the Information Systems were exchanging data with only one Information System. On average each Information System was indicated to be interoperable with at least one distinct Information System.

5.2.1.3 Information Systems' Interoperable Maturity

The summarized data from Table 5.3 and section C.1 in Appendix C served as the basis to assess the level of Information Systems' interoperability sophistication attained by each pair of technical interoperable Information Systems. The following pairs of unique Interoperable Information Systems were analysed:

- **Pair 1 (P1):** ASYCUDA and IFMS;
- **Pair 2 (P2):** DSA and IFMS;
- **Pair 3 (P3):** ECO and FIMS;
- **Pair 4 (P4):** GGFS and IFMS;
- **Pair 5 (P5):** GPS and IFMS;
- **Pair 6 (P6):** HRIMS and GPS;
- **Pair 7 (P7):** IRS and IFMS;
- **Pair 8 (P8):** MSS and FIMS;
- **Pair 9 (P9):** NPAS and NPRS;
- **Pair 10 (P10):** RESDAT and FIMS;
- **Pair 11 (P11):** SWS and IFMS; and
- **Pair 12 (P12):** VETS and IFMS.

The data for the unique pairs of interoperable Information Systems was analysed using the instruments of ISIMM (see Section 3.5.4). The results of the data analysis are presented in Table 5.4.

Table 5.4: Summary of Information Systems' Pairs Interoperability Compliancy

Codes	Layers/ Attributes	Information Systems Pairs											
		P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**	**P11**	**P12**
D	**Data Interoperability**	**2**	**2**	**4**	**2**	**2**	**3**	**2**	**3**	**3**	**3**	**2**	**2**
1	Common Data Presentation Format	X	X	X	X	X	X	X	X	X	X	X	X
2	Shared Meta Content												
3	Common Data Model			X			X						
4	Data Security	X	X	X	X	X	X	X	X	X	X	X	X
5	Shared Data			X					X	X	X		
S	**Software Interoperability**	**3**	**3**	**3**	**3**	**3**	**0**	**3**	**3**	**3**	**2**	**0**	**0**
1	N-Tier Interoperability Architecture	X	X	X	X	X		X	X	X	X		
2	Data Exchange Services	X	X	X	X	X		X	X	X	X		
3	Directory Services												
4	Common Naming Services												
5	Discovery Services												
6	Common Workflow Services												
7	Security Management Services	X	X	X	X	X		X	X	X			
8	Shared Applications												
C	**Communication Interoperability**	**1**	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**0**	**0**	**0**
1	Common Communication Protocols	X	X	X	X	X		X	X	X			
P	**Physical Interoperability**	**1**	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**0**	**0**	**0**
1	Shared Communication Network	X	X	X	X	X		X	X	X			

Table 5.4 is based on the Information Systems' Interoperability Maturity and Functional Compliancy Matrix (see Table 3.4). The attributes that each pair of interoperable Information Systems complies with are indicated with an 'X' in Table 5.4. The total number of attributes complied with for each interoperability layer is indicated in rows D, S, C and P of Table 5.4.

Table 5.5: Summary of Information Systems' Pairs Interoperability Layer Maturity Ratings and Scores

Codes	Layers/ Attributes	Information Systems Pair Ratings												Average Ratings
		P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**	**P11**	**P12**	
D	Data Interoperability	1E (2)	1E (2)	3E (4)	1E (2)	1E (2)	1E (3)	1E (2)	4E (3)	1E (3)	1E (3)	1E (2)	1E (2)	1A (2.5)
S	Software Interoperability	3B (3)	3B (3)	3B (3)	3B (3)	3B (3)	1E (0)	3B (3)	3B (3)	3B (3)	2E (2)	1E (0)	1E (0)	2E (2.1)
C	Communication Interoperability	2A (1)	2A (1)	2A (1)	2A (1)	2A (1)	1E (0)	2E (1)	2E (1)	2E (1)	1E (0)	1E (0)	1E (0)	2B (0.67)
P	Physical Interoperability	3E (1)	3E (1)	3E (1)	3E (1)	3E (1)	1E (0)	3E (1)	3E (1)	3E (1)	1A (0)	1A (0)	1A (0)	2E (0.67)
Totals:		**2A (7)**	**2A (7)**	**3E (9)**	**2A (7)**	**2A (7)**	**1E (3)**	**2A (7)**	**3B (8)**	**3B (8)**	**2B (5)**	**1E (2)**	**1E (2)**	**2E (6)**

Table 5.5 provides a summary of Information Systems' interoperability layer (see Section 4.3) based maturity ratings (e.g., 1E, 3E, 2A, 2E) and scores (e.g., 0, 2, 4, 6, 8) for each pair of interoperable Information Systems. The maturity level ratings per interoperability layer were determined by comparing the attribute scores on each interoperability layer of Table 5.4 with the interoperability layer compliance scores indicated in ISIMM (see Table 3.5). The rating codes used for each interoperability layer are defined in Table 3.6 of ISIMM.

From the analysis of Table 5.5, the following were derived for each pair of technical interoperable Information Systems:

(1) Pair P3 has the highest level of 'Data Interoperability' maturity;

(2) Pairs P1, P2, P3, P4, P5 have the highest level of 'Software Interoperability' maturity;

(3) Pairs P1, P2, P3, P4 and P5 have the highest level of 'Communication Interoperability' maturity; and

(4) Pairs P1, P2, P3, P4, P5, P7, P8 and P9 have the highest level of 'Physical Interoperability' maturity.

From Table 5.5 the average level of maturity per interoperability layer attained by Information Systems pairs was as follows:

(1) 'Data Interoperability' was at the 'Manual' level (Level 1) of maturity;

(2) 'Software Interoperability' was at the 'Ad-hoc' level (Level 2) of maturity;

(3) 'Communication Interoperability' was at the 'Ad-hoc' level (Level 2) of maturity; and

(4) 'Physical Interoperability' was at the 'Ad-hoc' level (Level 2) of maturity.

Table 5.6: Summary of Information Systems' Pairs Interoperability Maturity

Information Systems Pairs	**Levels/Degrees of Information Systems' Interoperability**				
	1:Manual	**2:Ad-hoc**	**3:Collaborative**	**4:Integrated**	**5:Unified**
P1		X			
P2		X			
P3			X		
P4		X			
P5		X			
P6	X				
P7		X			
P8			X		
P9			X		
P10		X			
P11	X				
P12	X				
Totals:	**3**	**6**	**3**		

The overall maturity position of each technical interoperable Information Systems' pairs is presented in Table 5.6. The maturity levels per pair of interoperable Information Systems were abstracted from Table 5.5.

Analysis of Table 5.6 indicates that three (25%) Information Systems' pairs were interoperable at interoperability maturity Level 1 (i.e., 'Manual' level) and that six Information Systems (50%) were technical interoperable at Level 2 (i.e., 'Ad-hoc' level) of maturity. Three (25%) Information Systems' pair was technical interoperable at Level 3 (i.e., 'Collaborative' level)

Overall the average level of interoperability maturity attained for interoperable pairs of Information Systems were at Level 2 (i.e., 'Ad-hoc' level).

5.2.2 Standards

The data obtained from interviewees indicated that no interoperability standards exist for the 12 technical interoperable Information Systems pairs studied. This finding correlates with the findings from the e-Government readiness survey conducted in 2011. The e-Government Readiness Report (GRN, 2011) indicated that Government Interoperability standards do not exist.

5.2.3 Data and Information

The data was analysed for the current presentation formats and data protection mechanisms used in exchanging data between interoperable Information Systems.

Table 5.7: Summary of Data Presentation Formats Used

No.	Presentation Form	Frequency	Percentage (%)
1	File (FILE)	8	66.67
2	Object (OBJ)	4	33.33
Totals:		**12**	**100**

Table 5.7 indicates that two different types of presentation formats were used to exchange data between the Information Systems cases studied. Predominantly 66.67% of Information Systems were exchanging data using 'Files' followed by data exchange through 'Objects' (33.33%).

Table 5.8: Summary of Data Protection Mechanisms Used

No.	Data Protection Mechanism	Total Identified	Percentage (%)
1	Hashing (HASH)	8	66.67
2	Authentication (ATH)	4	33.33
3	Authorization (AUT)	4	33.33

From Table 5.8, three different mechanisms were used to protect the data that was exchanged between Information Systems. 'Hashing' (66.67%) was indicated to be the most predominant protection mechanism, followed by 'Authentication' (33.33%) and 'Authorization' (33.33%).

5.2.4 Infrastructure

Data was analysed for the current forms of interoperability architectures employed, services offered, exchange protocols and network topology used in establishing technical interoperability.

Table 5.9: Summary of Interoperability Architectures Used

No.	Interoperability Architecture	Total Identified	Percentage (%)
1	Client-Server Architecture (CSA)	9	75
2	No Architecture (NONE)	3	25

Table 5.9 indicates that only one type of interoperability architectures were used to exchange data between Information Systems. Most organisations used the 'Client-Server Architecture' form of architecture (75%). Interviewees indicated that 25% of data exchanges between Information Systems were not through any data exchange architecture.

Table 5.10: Summary of Interoperability Related Services Provided

No.	Services	Total Identified	Percentage (%)
1	Security Management Services (SMS)	9	75.00
2	Data Import and Export Services (DIES)	8	66.67
3	File Transfer Services (FTS)	5	41.67
4	Transactional Services (TRS)	4	33.33

From Table 5.10, four different types of interoperability related services were found to be offered by interoperable Information Systems through their interoperability architectures. From Table 5.10, 'Security Management Services' (75%) was indicated to be the most provided service, followed by 'Data Import and Export Services' (66.67%) and 'File Transfer Services' (41.67%). The least provided service by interoperable Information Systems is 'Transactional Services' (33.33%).

Table 5.11: Summary of High Level Data Exchange Protocols Used

No.	Protocols	Total Identified	Percentage (%)
1	File Transfer Protocol (FTP)	5	41.67
2	Vendor Specific Protocol (VSP)	4	33.33
3	No protocol (NONE)	3	25.00

From table 5.11, three different types of high level data exchange protocols were used to exchange data between Information Systems. The protocol 'File Transfer Protocol' (41.67%) was primarily used followed by the 'Vendor Specific Protocol' (33.33%) group of protocols. Table 5.11 also indicates that 25% of data exchanges were made using no protocols. These exchanges were through physical data exchange means.

Table 5.12: Summary of Communication Network Types Used

No.	Services	Frequency	Percentage (%)
1	Local Area Network (LAN)	8	66.67
2	No Network (NONE)	3	25
3	Wide Area Network (WAN)	2	16.67

Table 5.12 indicates that two types of networks were used to connect interoperability Information Systems. Most organisations used their 'Local Area Network' (66.67%) to exchange data. A total of 25% of the Information Systems used no network to exchange data whereas 'Wide Area Network' (16.67%) was indicated to be the least used network type for exchanging data.

5.3 Required State of Interoperability

The data gathered was analysed based on the interviewees' perceptions of their required future data and technical interoperability state. The combined and summarized data utilized in this section is located in section C.2 of Appendix C.

5.3.1 Collaboration

The analyses of the data gathered from interviewees are presented in this section for the required data sharing collaborations to be established between organisations and their Information Systems. The analysis includes comparisons between the current and required states of interoperability as well as an analysis of the degree of Information Systems' maturity sophistication desired.

5.3.1.1 Organisational Collaboration

Interviewees' indicated that there was a need to increase interoperability between organisations and within organisations themself. Table 5.13 shows the degree to which public service organisations would like to form collaborations.

Table 5.13: Summary of Collaborations Required between Organisations

Rank Order	Organisations	Data Exchange Partners		
		Internal	**Public Service**	**Total**
1	Ministry of Finance (MOF)	1	10	11
1	Office of the Prime Minister (OPM)	1	10	11
2	Ministry of Home Affairs and Immigration (MHAI)	1	7	8
3	Ministry of Lands, Resettlement and Rehabilitation (MLRR)	1	2	3
3	Ministry of Justice (MOJ)	1	2	3
4	Ministry of Fisheries and Marine Resources (MFMR)	1	1	2
4	Ministry of Labour and Social Welfare (MOLSW)		2	2
4	Ministry of Veterans' Affairs (MOVA)		2	2
4	Ministry of Trade and Industry (MTI)		2	2
5	Ministry of works and Transport (MWT)		1	1
Totals:	**10**	**6**	**39**	**45**
Average:		**0.6**	**3.9**	**4.5**

Analysis of Table 5.13 indicates that there is a need to establish data sharing partnerships between ten organisations. From Table 5.13, the largest number of partnerships required was with the 'Ministry of Finance' (10) and the 'Office of the Prime Minister' (10). The organisation with the lowest indicated data exchange partnership requirement was the 'Ministry of Works and Transport' (1). On average there is a need to exchange data with at least four organisations.

Figure 5.2 provides a comparison of the different sectors of data exchange collaboration between organisations for the current and the required future situation.

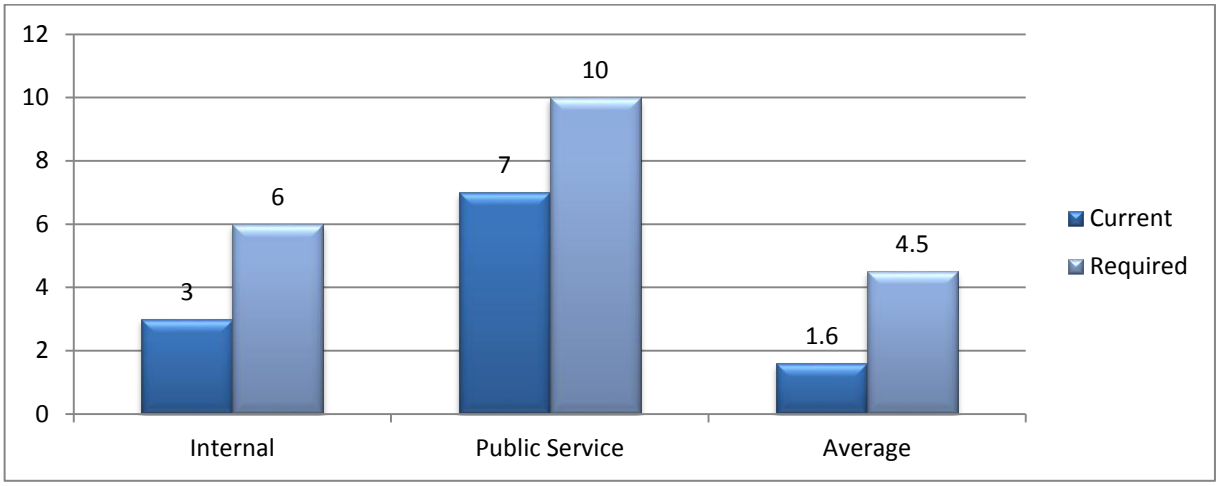

Figure 5.2: Bar Chart of Organisational Sector Collaborations Comparisons by Number of Interconnections

From Figure 5.2, there is need to increase the number of internal data exchange collaboration within organisations from three to six and collaboration between public service organisations from seven to ten organisations. On average there is a need to increase collaboration between organisations from one to four organisations.

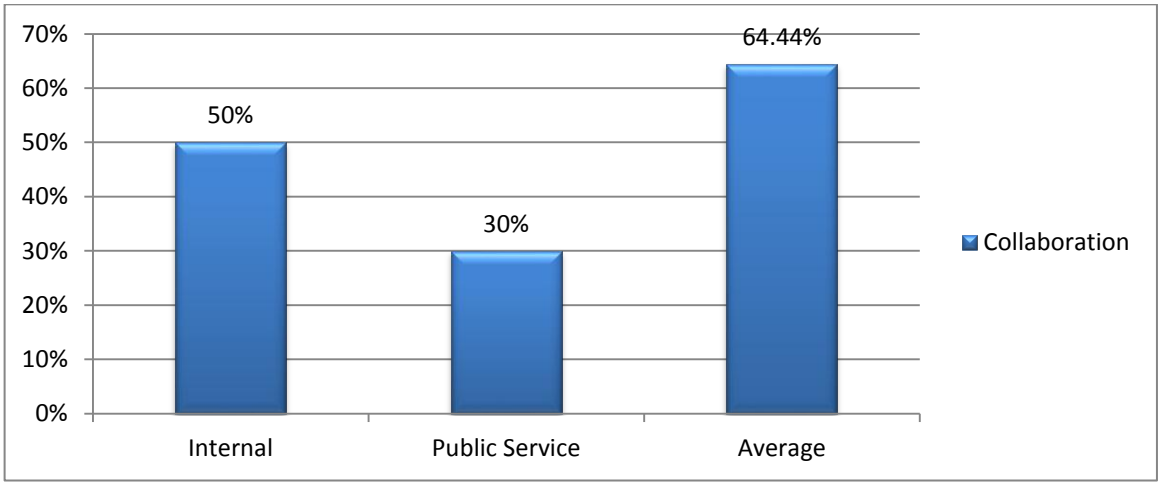

Figure 5.3: Bar Chart of Organisational Sector Collaborations by Percentage of Interconnection Increase

The percentage increase in collaboration required within and between organisations is presented in Figure 5.3 for the different sectors of collaboration. From Figure 5.3, internal (50%) collaboration indicates the highest required increase in collaboration followed by Public Service (30%) collaboration. On average an increase in collaboration of 64.44% is required for both intra-organisational and inter-organisational data exchange.

5.3.1.2 Technical Interoperable Information Systems

Data from the interview results were analysed based on the current and required technical interoperable between Information Systems.

Table 5.14 compares the number of technical interoperable Information Systems for the current and the required future situation.

Table 5.14: Summary of Technical Interoperable Information Systems

Current State	Required State	Percentage Increase
15	22	31.82%

From Table 5.14, interviewees indicated that there was a need to increase interoperability between Information Systems by 31.82% from 15 to 22 interoperable Information System.

5.3.1.3 Information Systems' Interoperable Maturity

The combined and summarized data from section C.2 in Appendix C served as the source to assess the overall level of interoperability sophistication required for Information Systems in the future. The data was analysed using the tools of ISIMM (see Section 3.5.4).

Table 5.15: Summary of Required Information Systems Technical Interoperability Compliancy

Code	Layers/Attributes	Compliancy Ratings
D	**Data Interoperability**	**5**
1	Common Data Presentation Format	X
2	Shared Meta-Content	X
3	Common Data Model	X
4	Data Security	X
5	Shared Data	X
S	**Software Interoperability**	**5**
1	N-Tier Interoperability Architecture	X
2	Data Exchange Services	X
3	Directory Services	X
4	Common Naming Services	
5	Discovery Services	
6	Common Workflow Services	
7	Security Management Services	X
8	Shared Applications	X
C	**Communication Interoperability**	**1**
1	Common Communication Protocols	X
P	**Physical Interoperability**	**1**
1	Shared Communication Network	X
Total:		**12**

Table 5.15 provides a summary of the attributes identified by interviewees that comply with the Information Systems' Interoperability Maturity and Functional Compliancy Matrix (see Table 3.4) attributes. The attributes identified by interviewees are indicated with an 'X' in Table 5.15.

Table 5.16: Summary of Required Information Systems Technical Interoperability Layer Maturity

Code	Layers/Attributes	Score	Compliancy Ratings
D	Data Interoperability	5	4E
S	Software Interoperability	5	4A
C	Communication Interoperability	1	4E
P	Physical Interoperability	1	4E
Overall:		**12**	**4E**

Indicated in Table 5.16 is a summary of the required technical interoperability layer (see Section 4.3) based maturity ratings for the Information Systems analysed. The ratings (e.g., 4E) for each interoperability layer are defined in Table 3.5 of ISIMM. The overall rating indicates that there was a need to achieve the 'Integrated' level (i.e., Level 4) of technical interoperability maturity compliance between Information Systems.

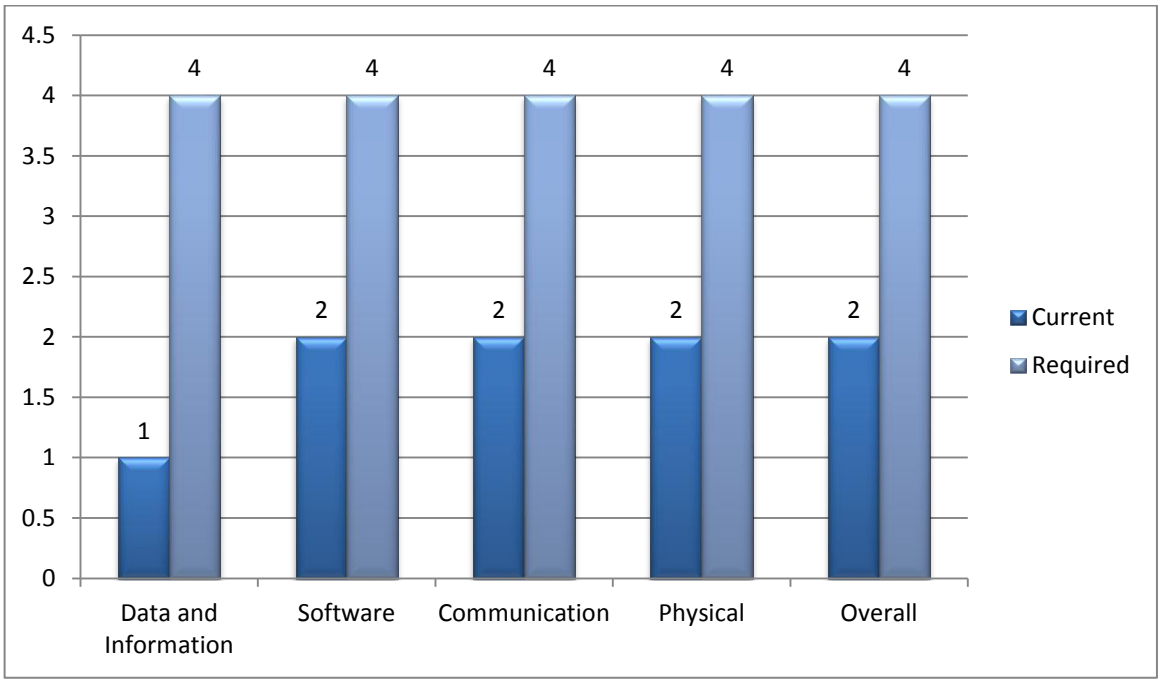

Figure 5.4: Bar Chart of Technical Interoperability Layer Comparisons by Maturity Compliancy Rating

The differences in technical interoperability maturity for the current and required states are presented in Figure 5.4. Figure 5.4 indicates that overall interviewees required that current interoperable Information Systems should move from a 'Ad-hoc' level (i.e., Level 2) of

interoperability sophistication to an 'Integrated' level (i.e., Level 4) of interoperability sophistication. The highest degree of interoperability advancement was required at the 'Data and Information' interoperability layer.

5.3.2 Standards

The responses obtained from the 26 interviewees indicated that 21 (80.77%) felt that interoperability standards were required and five (19.23%) felt that there was no need for interoperability standards. The e-Government Readiness Report (GRN, 2011) indicated that interoperability standards were under discussion with the purpose to establish appropriate interoperability standards.

5.3.3 Data and Information

The data was analysed for the presentation formats and data protection mechanisms required to exchanging data between interoperable Information Systems.

Table 5.17: Summary of Data Presentation Formats Required

No.	Presentation Form	Total Identified	Percentage (%)
1	File (FILE)	25	96.15
2	Extensible Mark-Up Language Text Format (XML)	23	88.46
3	Object (OBJ)	11	42.31

Table 5.17 indicates that three different types of presentation formats were required to exchange data between Information Systems. The 'File' (96.15%) data presentation format was required by most followed by 'Extensible Mark-Up Language Text Format' (88.46%) format. The data presentation format least indicated by interviewees was 'Object' (42.31%).

Table 5.18: Summary of Data Protection Mechanisms Required

No.	Data Protection	Total Identified	Percentage (%)
1	Authentication (ATH)	26	100.00
2	Hashing (HASH)	21	80.77
3	Authorization (AUT)	20	76.92
4	Encryption (ENC)	17	65.38

From Table 5.18, four different mechanisms were identified to protect data exchanges between Information Systems in the future. 'Authentication' (100%) was indicated to be the most dominant protection mechanism required, followed by 'Hashing' (80.77%). The least indicated protection mechanism required by interviewees was 'Encryption' (65.38%).

5.3.4 Infrastructure

Data was analysed for the interoperability architecture forms, services offered, exchange protocols and network topology required in the future.

Table 5.19: Summary of Interoperability Architecture Forms Required

No.	Interoperability Architecture	Total Identified	Percentage (%)
1	Client-Server Architecture (CSA)	19	73.08
2	Service Oriented Architecture (SOA)	14	53.85
3	Peer-to-Peer Architecture (PPA)	8	30.77

Table 5.19 indicates three different required types of interoperability architectures identified to share data between Information Systems. Most interviewees indicated the 'Client-Server Architecture' (73.08%) followed by the 'Service Oriented Architecture' (53.85%) form. The least indicated architectural form by interviewees was the 'Peer-to-Peer Architecture' (30.77%).

Table 5.20: Summary of Interoperability Related Services Required

No.	Services	Total Identified	Percentage (%)
1	Data Import and Export Services (DIES)	25	96.15
2	File Transfer Services (FTS)	25	96.15
3	Security Management Services (SMS)	22	84.62
4	Web Services (WS)	22	84.62
5	Remote Procedure Calls (RPC)	16	61.54
6	Transactional Services (TRS)	11	42.31
7	Data Replication Services (DRS)	6	23.08

From Table 5.20, seven different types of interoperability related services were required to be offered by interoperable Information Systems through their interoperability architectures. Table 5.20 shows that 'Data Import and Export Services' (96.15%) and 'File Transfer Services' (96.15) were required by most, followed by 'Security Management Services' (84.62%) and 'Web Services' (84.62%). The interoperability related service least required was 'Data Replication Services' (23.08%).

Table 5.21: Summary of High Level Data Exchange Protocols Required

No.	Protocols	Total Identified	Percentage (%)
1	File Transfer Protocol (FTP)	25	96.15
2	Hypertext Transmission Protocol (HTTP)	23	88.46
3	Vendor Specific Protocol (VSP)	15	57.69

From table 5.21, three different types of high level data exchange protocols were required to exchange data between Information Systems via their interoperability architecture. The 'File Transfer Protocol' (96.15%) was primarily required followed by the 'Hypertext Transmission Protocol' (88.46%). The least required data exchange protocol indicated by interviewees was the 'Vendor Specific Database Protocol' (57.69%) group of protocols.

Table 5.22: Summary of Communication Network Types Required

No.	Services	Total Identified	Percentage (%)
1	Local Area Network (LAN)	26	100
2	Wide Area Network (WAN)	26	100

Table 5.22 indicates that two different types of networks were required to connect interoperability Information Systems. All interviewees indicated that both 'Local Area Network' (100%) and 'Wide Area Network' (100%) connections were required for communication between and among public service organisations.

5.4 Interoperability Adoption Factors

The data to be analysed is the factors that influence the adoption of interoperability that was gathered from interviewees. The data analysis was based on the interviewees' perceptions of interoperability adoption in the GIGF domains of: (a) Collaboration, (b) Standards, (c) Data and Information, and (d) Infrastructure. The data utilized is located in section C.3 of Appendix C.

Through the analysis of the interview results in Appendix C, 11 different common related interoperability adoption factors were identified within the four GIGF interoperability domains. Table 5.23 present a summary of the adoption factors identified by interviewees for each of the GIGF domains.

Table 5.23: Interoperability Adoption Factors per GIGF Domain

Domains	**Technical Interoperability Adoption Factors**	**Number of Factors**	**Percentage (%)**
Collaboration	Agreements, Management support and Policies.	3	12.5
Standards	Appropriate, Collective Agreements and Understandable.	3	12.5
Data and Information	Availability, Accountability, Restrictions, Standards, Quality and Security.	6	25
Infrastructure	Availability, Compatibility, Connectivity, Cost, Ease of use, Flexibility, Hosting platforms, Performance, Restrictions, Security, Skills and Standards	12	50
Total:		**24**	**100**

The common interoperability adoption factors in Table 5.22 where used as the variables for summaries, frequencies and correlations presented in this section.

Analysis of the data in Table 5.23 indicates that the domains of ‘Infrastructure’ (50%) and ‘Data and Information’ (25%) had the most identified interoperability adoption factors, followed by the domains ‘Collaboration’ (12.5%) and ‘Standards’ (12.5%). Interviewees also indicated that the ‘Infrastructure’ domain had the largest number of identified (12) technical interoperability adoption factors, with the domains of ‘Collaboration’ (3) and ‘Standards’ (3) having the lowest.

5.4.1 Cross Domain Frequency Analysis

Table 5.24 presents a rank order summary of the seven most identified technical interoperability adoption factors across all GIGF domains (see Appendix C) by interviewees.

Table 5.24: Interoperability Adoption Factors Identified

Rank Order	Technical Interoperability Adoption Factors	Total Identified	Percentage (%)
1	Data Security	26	100
2	Data Quality	22	84.62
3	Connectivity	21	80.77
4	Performance	20	76.92
4	Infrastructure Security	20	76.92
5	Accountability	19	73.08
6	Compatibility	18	69.23

The 'Total Identified' column in Table 5.24 indicates the number of interviewees that identified the factor.

Table 5.25: Keyword Frequencies of Interoperability Adoption Factors

Rank Order	Technical Interoperability Adoption Factors	Frequencies
1	Data Security	33
2	Data Quality	30
3	Accountability	27
3	Connectivity	27
4	Infrastructure Security	26
5	Performance	25
6	Compatibility	23

Table 5.25 presents a rank ordered summary of the most used interoperability adoption factor keywords by interviewees. Analysis of the data in Table 5.25 indicates that interoperability adoption factor 'Data Security' had the highest frequency of occurrence with 'Compatibility' having the lowest frequency of occurrence.

5.4.2 Means and Standard Deviations

The mean and standard deviation descriptive statistics are presented in Table 5.26 for the interoperability adoption factor (variable) keywords.

Table 5.26: Interoperability Adoption Factors Means and Standard Deviation

Variables	N	Means	Standard Deviations
Data Security	26	1.27	0.60
Data Quality	26	1.15	0.73
Connectivity	26	1.04	0.72
Compatibility	26	0.88	0.59
Performance	26	0.96	0.72
Infrastructure Security	26	1.00	1.02
Accountability	26	1.04	1.11

The standard deviations in Table 5.26 indicate that 85% of values are normally distributed and lie between one standard deviation below and one standard deviation above the mean. The assumption can thus be made that the variables are approximately normally distributed, and this makes it suitable for use in testing relationships.

5.4.3 Relationships

The Pearson product-moment correlation was used to determine if significant relationships existed between different combinations of variables. The variables consisted of the interoperability adoption factors that were most frequently stated by interviewees (see Table 5.26). Correlations where tested by comparing and contrasting different combinations of variables.

The four statistical significant correlations identified between the different variable combinations are presented in Table 5.27.

Table 5.27: Interoperability Adoption Factors Correlation Matrix

Variables	Connectivity	Infrastructure Security	Accountability
Data Security	r = 0.53; p = 0.006		
Data Quality			r = 0.48; p = 0.012
Compatibility		r = -0.53; p = 0.005	

A number of significant relationships where also identified (see Section 5.2.4.3) for the following dependant and independent variable combinations:

- ‘Data Security’ and ‘Connectivity’ where found to be statistically significantly correlated at the 1% level (r=0.53; p=0.006).
- ‘Compatibility’ and ‘Infrastructure Security’ where found to be statistically significantly correlated at the 1% level (r=0.53; p=0.005).
- ‘Accountability’ and ‘Data Quality’ where found to be statistically significantly correlated at the 5% level (r=0.48; p=0.012).

The highest significant level of correlation was found between the variables ‘Data Security’ and ‘Connectivity’. The lowest significant level of correlation was indicated as the variables ‘Accountability’ and ‘Compatibility’.

5.5 Summary

The analyses of the data gathered from interviewees were presented in this chapter in three sections. The data analysis focussed on the interviewee’s perceptions of the current technical interoperable situation, perceived future interoperability needs and the factors that may impact interoperability adoption within the public service.

The next chapter will focus on answering the research questions in relationship to the analysis findings of the current state of interoperability, required state of interoperability and the factors that may influence interoperability adoption within the public service.

6. DISCUSSION OF DATA ANALYSIS FINDINGS

In this chapter, the research questions posed in this thesis are answered through the discussion of the data analysis findings. The chapter discusses the findings for each research question separately and concludes with a brief chapter summary.

6.1 Introduction

The data analysis presented in Chapter 5 for the current technical interoperability state, required technical interoperability state and adoption factors will be discussed in this chapter in relation to the research questions posed in this thesis.

6.2 Research Question One: "Which forms of technical interoperability exist within the Public Service of Namibia?"

The information source for research question one is the data analysis conducted for the current state of technical interoperability within the Public Service. The results of the data analysis are recorded in Section 5.2 of Chapter 5.

The data analysis results of Section 5.2 show that a small number of public service organisations were collaborating. Data sharing and data exchange between most Information Systems was mostly inter-organizationally focussed, followed by intra-organizational interoperability. The data analysis results also indicate that no interoperability standards existed for sharing or exchanging of data between public service organisations.

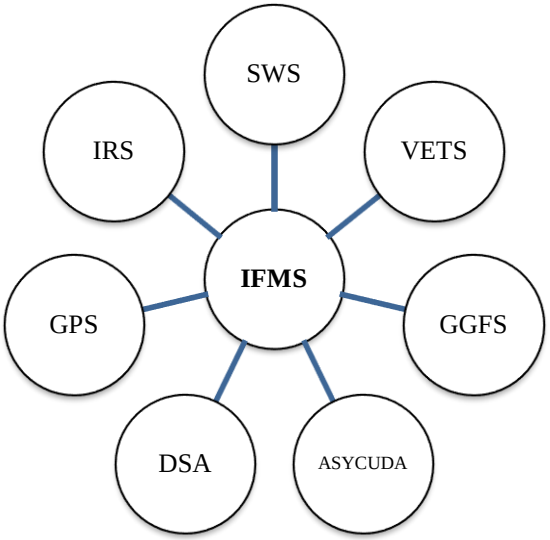

Figure 6.1: Finances Sector Based Cluster

The analysis of the data findings shows that Information Systems were sharing and exchanging data in a number of small public service policy (e.g., finance) sector based clusters. The Information Systems within these clusters were connected to a central Information System (e.g., Figure 6.1) forming a star type topology. The finances sector cluster was found to be the largest of these public service policy sector based clusters, consisting of eight Information Systems connected to the Integrated Financial Management System (IFMS) (see Figure 6.1) at the Ministry of Finance.

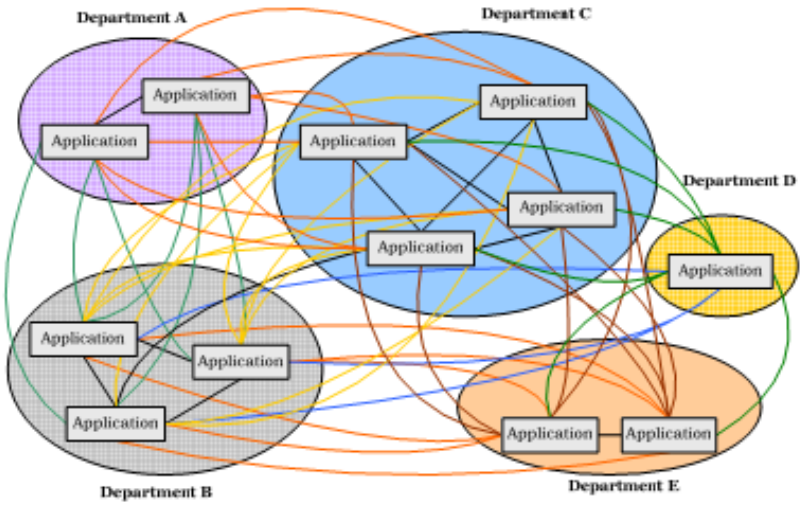

Figure 6.2: Point-to-point (Bilateral) Connection Topology with Multiple Information Systems Connections

Information Systems were found to be cross connected between clusters forming multiple bilateral connections (see Figure 6.2). This interconnection situation creates a **n(n-1)/2** potential interconnection problem. According to IDBC (2004) and Lallana (2008), bilateral (point-to-point) architectures as established by the public service pose a number of problems such as:

(1) Point-to-point connections does not scale well as more and more bilateral exchanges are required and new connections are required to additional Information Systems.
(2) Point-to-point connections are costly to develop and maintain as each bilateral exchange needs to be custom developed for each data exchange.
(3) Point-to-point connections do not accommodate common or aggregated data or services.

From the data analysis results it was further gathered that interoperability between pairs of Information Systems was at a low level of Information Systems' interoperability sophistication. The analysis also indicted that the majority of Information System pairs were exchanging data using basic data exchange mechanisms (e.g., file transfer) or by connecting directly to the databases that hosted the data.

The results from the analyses shows that interoperability of distinct pairs of Information Systems was at different levels of technical interoperability maturity sophistication, alternating between Level 1 ('Manual' level), Level 2 ('Ad-hoc' level) and Level 3 ('Collaborative' level) of Information Systems' interoperability maturity (see Section 5.2.1.3). The overall degree of technical interoperability maturity attained by the Information Systems analysed was either at Level 1 ('Manual' level) or Level 2 ('Ad-hoc' level) of interoperability maturity (see Section 5.2.1.3). However, the data analysis

findings indicated that different levels of maturity were attained for each form of technical interoperability by Information Systems exchanging data.

Table 6.1: Summary of Technical Interoperability Layers, Domains and Attributes (Current State)

Interoperability Layers and Domains	**Attributes**
4-Data Interoperability	
Common Data Presentation Formats	• File • Object
Data Security	• Authentication • Authorization • Hashing
3-Software Interoperability	
N-Tier Common Interoperability Architecture	• Client-server
Services	• Data Import and Export Services • File Transfer Services • Security Management Services • Transactional Services
2-Communication Interoperability	
Common Communication Protocols	• FTP • VSP
1-Physical Interoperability	
Shared Communication Network	• LAN • WAN

Table 6.1 provides a summary of the technical interoperability attributes identified through the data analysis for each of the four technical interoperability domains (see Section 5.2 of Chapter 5) that form part of the interoperability systems architectures utilised at present.

From the data analysis results it was established that at an architectural level Information Systems were predominantly organised according to the Client-Server Architectural model. Client-server type technologies were used primarily to transfer files and perform database transactions. None of the newer types of systems architectures (e.g., Web based

Architecture, Service Oriented Architecture, Collaboration Architecture) or data sharing services available for sharing service or exchanging data were employed by any of the public service organisations.

In summary, technical interoperability was attained at different levels of sophistication within the different forms of technical interoperability as follows:

(1) Interoperability of data was attained at Level 1 (‘Manual’ level) of technical maturity.
(2) Interoperability of software was attained at Level 2 (‘Ad-hoc’ level) of technical maturity.
(3) Interoperability of communications was attained at Level 2 (‘Ad-hoc’ level) of technical maturity.
(4) Interoperability of physical devices was attained at Level 2 (‘Ad-hoc’ level) of technical maturity.

Overall, technical interoperability between Information Systems was of an ‘Ad-hoc’ (Level 2) interoperability form and based on the client-server systems architecture model.

6.3 Research Question Two: “What forms of models will be required to establish technical interoperability within the Public Service of Namibia?”

The information source for research question two is the data analysis conducted for the required state of technical interoperability within the public service. The results of the data analysis are recorded in Section 5.3 of Chapter 5.

The data analysis findings indicated that there was a need to expand the current level of collaborations within public service organisation and within the public service (see Section 5.3.1.1). The data analysis findings also indicated that there was a need to drastically expand the number of technical interoperable Information Systems and to advance the

interoperability sophistication of technical interoperability between interoperable environments (see Section 5.3.1.2).

The data analysis findings indicated that the largest number of collaboration partnerships were required internally within public service organisations followed by intra public service collaboration. The data analysis results suggest that connections between Information Systems need to increase by 64.44%.

On average Information Systems interoperability was required at different levels of Information Systems' interoperability sophistication (see Section 5.3.1.3) for each of the different forms of technical interoperability as follows:

(1) Interoperability of data was required at Level 4 ('Integrated' level) of technical maturity.
(2) Interoperability of software was required at Level 4 ('Integrated' level) of technical maturity.
(3) Interoperability of communications was required at Level 4 ('Integrated' level) of technical maturity.
(4) Interoperability of physical devices was required at Level 4 ('Integrated' level) of technical maturity.

Overall, technical interoperability for the four layers of technical interoperability maturity was required at the 'Integrated' level (Level 4) of maturity.

Table 6.2: Summary of Technical Interoperability Layers, Domains and Attributes (Required State)

Interoperability Layers and Domains	**Attributes**
4-Data Interoperability	
Common Data Presentation Formats	• File • XML • Object
Data Security	• Authentication • Authorization • Encryption • Hashing
3-Software Interoperability	
N-Tier Common Interoperability Architecture	• Client-Server Architecture • Service Oriented Architecture (SOA) • Peer-to-Peer Architecture
Services	• Data Import and Export Services • Data Replication Services • File Transfer Services • RPC Services • Security Management Services • Transactional Services • Web Services
2-Communication Interoperability	
Common Communication Protocols	• FTP • HTTP • VSP
1-Physical Interoperability	
Shared Communication Network	• LAN • WAN

Table 6.2 provides a summary of the technical interoperability attributes within the four technical interoperability domains desired by interviewees for the technical interoperability architecture of the future. The attributes of Table 6.2 were abstracted from required state of interoperability findings as presented in Section 5.3 of Chapter 5.

At an architectural level, interviewees indicated three different types of systems architectures to exchange data namely: (a) Client-Server Architecture, (b) Service Oriented Architecture and (c) Peer-to-Peer Architecture. Seven services were also identified that had to be provided by the systems architectures identified such as: (a) Data Import/Export Services, (b) Data Replication Services, (c) File Transfer Services, (d) Remote Procedure Calls, (e) Security Management Services, (f) Transactional Services, and (g) Web Services.

The protocols of FTP, HTTP and VSP were indicated by interviewees' as the preferred protocols for exchanging data between interoperability partners. Interviewees' indicated that data exchange between partners should make use of File, XML and Object data presentation formats.

The architectural forms, services, protocols and presentation formats identified by interviewees indicates that a hybrid distributed systems architectural style will be required that includes architectural style characteristics of the layered, object and event based distributed systems architectural styles (see Section 2.4).

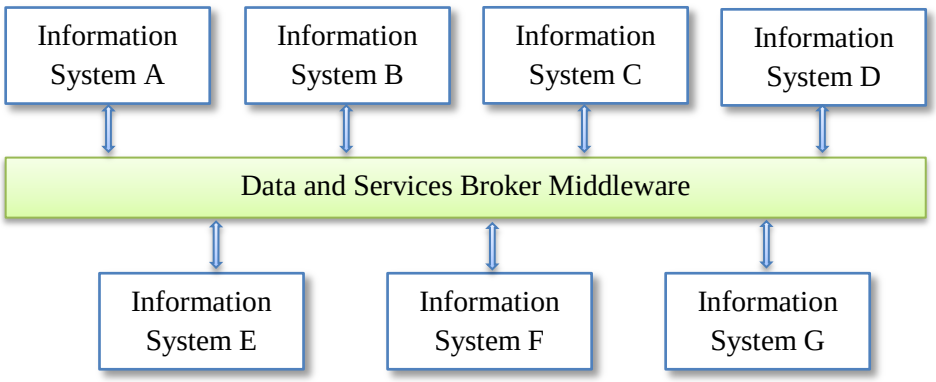

Figure 6.3: Data and Services Exchange Architecture Configuration

Based on the data analysis findings, the public service requires a hybrid interoperability form of systems architecture model that includes the characteristics the client-server, peer-to-peer and service oriented distributed systems architectural forms (see Section 2.4).

To establish and maintain interconnections and interactions between Information Systems, the hybrid interoperability systems architecture will need to function in part as a middleware layer (see Figure 6.3) in line with the Government of Namibia's policy directives identified in section 2.7. The middleware layer of Figure 6.3 connects heterogeneous Information Systems and provides services to these Information Systems that will allow them to interact and exchange data. The use of a middleware layer provides a number of advantages such as:

(1) Masks the heterogeneity of the underlying network, hardware and Information Systems (Coulouris et al., 2009);
(2) Provides a convenient programming model (Coulouris et al., 2009);
(3) Decreases the dependency of applications on a particular operating system and increases the ease of moving applications to new computers or systems (Schimdt & Lyle, 2010);
(4) Provides distributed transparency (Tanenbaum et al., 2007); and
(5) Easy to configure, adopt and customize (Tanenbaum et al., 2007);

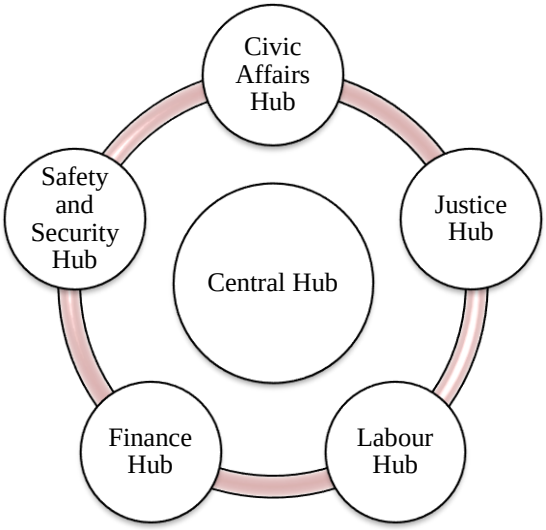

Figure 6.4: Hub-and-spoke Connection Topology for Public Service Sectorial Clusters

To solve the bilateral connection problem as identified in Section 6.2, a hub-and-spoke type topology as shown in Figure 6.4 is proposed. The hub-and-spoke type topology provides the mechanisms to establish multilateral agreements between different sectorial clusters in a connection efficient manner. The end nodes of the hub-and-spoke topology serve to connect together Information Systems from the same public service sector (e.g., Finance, Justice). The end nodes intern is connected to the central hub (see Figure 6.4) which will facilitate cross sector data exchange.

In summary, the hybrid interoperability architectural model required will need to provide the services identified by interviewees, comply with policy directives and accommodate the legacy infrastructure and software already present within the public service. Technical interoperability factors that may influence the adoption of the architectural model should also be addressed as far as possible by the interoperability architectural model design. The proposed interoperability architectural model is discussed in Chapter 7.

6.4 Research Question Three: "What factors will influence the adoption of interoperability within the Public Service of Namibia?"

The information source for research question three is the data analysis conducted for the technical interoperability factors identified which was recorded in Section 5.4 of Chapter 5. The findings and conclusions are presented below for this question.

From the data analyses results, 24 distinct interoperability adoption factors were identified that will influence the establishing of interoperability within the public service. From the 24 interoperability adoption factors identified, the seven most identified interoperability adoption factors (see Section 5.4.1) are the following:

(1) **Data Security:** Interoperability solutions should ensure protection of data within hosting environments and data in-use within applications.

(2) **Data Quality:** Data to be shared among Information Systems should be accurate, precise, complete, usable and consistent.

(3) **Connectivity:** Before data exchange can take place between Information systems, physical interoperability (e.g., LAN and WAN) should be established between systems.

(4) **Compatibility:** Hardware and software should be designed or made to be compliant with each other.

(5) **Performance:** Interoperability solutions should provide acceptable throughput and response times for all data requests made between systems.

(6) **Infrastructure Security:** Infrastructure should protect data in motion and at rest, ensuring data confidentially, integrity and availability (i.e., CIA).

(7) **Accountability:** A person or organisation should be made and held responsible for the upkeep and protection of data provided to other users.

Three notable statistical significant correlations where also found between different interoperability adoption factor variables. The correlations suggest that ‘Data Security’ plays a major role in the ‘Connectivity’ of Information Systems. The correlations identified further suggest that ‘Accountability’ plays a role in ‘Data Quality’ and that ‘Compatibility’ plays a role in the form of ‘Infrastructure Security’ established. The identified correlations are not necessarily cause-effect correlation relationships.

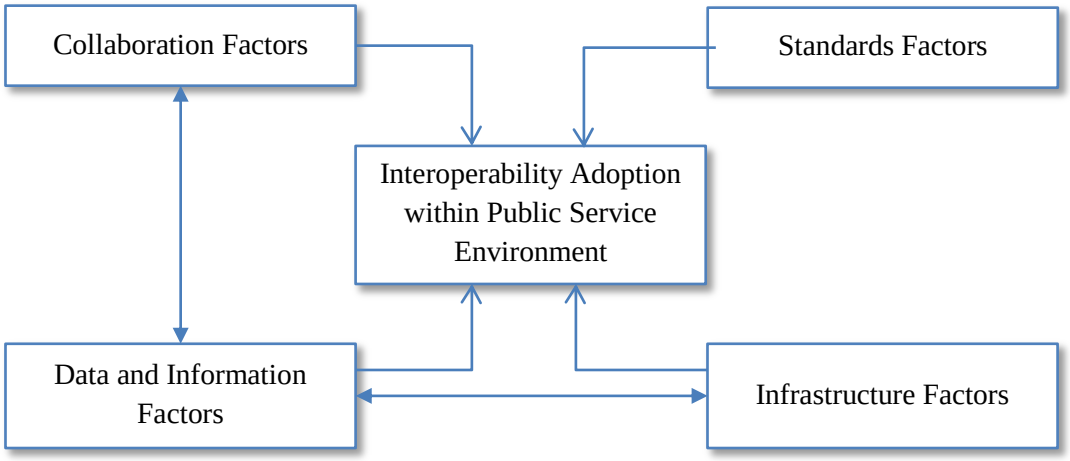

Figure 6.5: Conceptual Model for Interoperability Adoption within the Public Service Environment

Figure 6.5 illustrates the conceptual model that was formulated from the data analysis findings. The model indicates the interoperability adoption factor domains and relationships between them. The model further shows that adoption factor domains will individually as well as collectively influence the establishing of interoperability within the public service.

In summary, the study showed that the adoption of interoperability within the public service will be influenced by a large number of factors within different domains of which a small number of factors were in correlation relationships with one another. The interoperability adoption factors identified have to be taken into account when examining the risk of establishing interoperability or when implementing an interoperability solution. The seven most identified interoperable adoption factors (see Section 5.4) potentially pose the highest risk to establishing interoperability within the public service.

6.5 Summary

The data analyses findings of Chapter 5 were discussed and presented in this chapter in relationship to the three research questions posed in this thesis. The following chapter will

discuss the interoperability architecture model created from the data analysis findings and relevant literature studied.

7. ARCHITECTURE MODEL TO ESTABLISH E-GOVERNMENT TECHNICAL INTEROPERABILITY WITHIN THE PUBLIC SERVICE

This chapter provides an analogy of the data found within the public service and discusses the Cooperative Architectural Model (CAM) that was developed to share and exchange data within the public service. The chapter concludes with a chapter summary.

7.1 Introduction

Historically, the Public Service of Namibia has deployment incoherent Information Systems that were developed along departmental or functional boundaries with little or no information sharing or information exchange among themselves (OPM, 2004), the foundation of the interoperability problem. Therefore, output and outcome are partial and it leads to the formation of information and Information Systems islands.

The establishing of interoperability between systems will be a key issue in unlocking data that is required to enable e-Government solutions. However, the sharing and exchanging of data among Information Systems will be constrained by the extent to which data has been duplicated within the Government as well as the manner in which it is distributed across Government institutions.

In this chapter, the Cooperative Architectural Model (CAM) is discussed which was developed to meet the technical compliancy complexities and data sharing and data exchange challenges of the Public Service of Namibia. The CAM in particular addresses the research aim of this study which is:

"To create a public service centred cooperative architectural model that defines and guides the establishing of technical interoperability within the context of the Public Service of Namibia".

The knowledge obtained in studying the current and required state of interoperability (see Chapter 5 and Chapter 6) in the Public Service and the relevant literature (see Chapter 2) formed the basis for the CAM design. In the development of CAM, consideration was also given to the interoperability adoption factors (see Section 6.4) that may pose a risk to the adoption of the CAM.

The CAM focuses on addressing three core issues identified such as:

(1) Data Sharing and Exchange: Enables the sharing and exchange of data between different Information Systems.

(2) Data Presentation: Focuses on the various means of exposing data through different access challenges in a standard manner.

(3) Interconnectivity: Enables communication between Information Systems.

The value of CAM is that it provides an architectural blueprint for achieving the Government's vision and policies; ensures alignment to business operations and efficiency of connections between public service organisations (i.e., interoperability) and reduces the duplication of assets and resources. The CAM furthermore provides the mechanism to utilise the current Public Service Information Systems environment while providing the mechanisms to move to the desired state of technical interoperability.

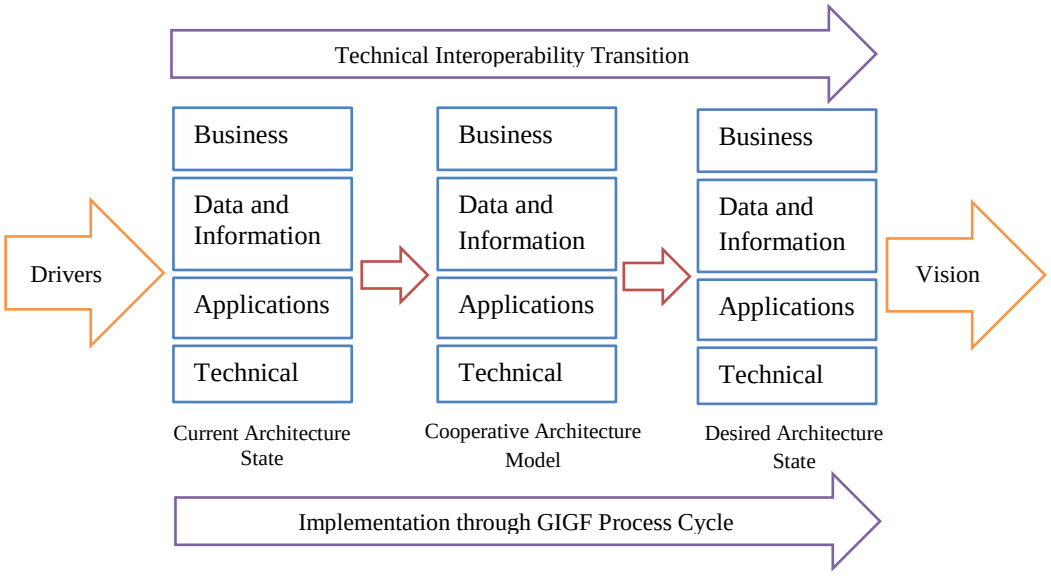

Figure 7.1: Architectural Model Transitional Process

The transitional process from the current interoperable state to the desired interoperability state is reflected in Figure 7.1.

The following sections will offer a viewpoint into the types of data found within an e-Government ecosystem and describe the different aspects of CAM that will facilitate the sharing and exchange of data within the Public Service of Namibia.

7.2 Analogy of Data within the e-Government Interoperable Ecosystem

From a research perspective, two types of data can be identified that can be gathered, namely: (a) primary data and (b) secondary data. Primary data constitutes data gathered directly from data sources whereas secondary data constitutes data gathered from existing data sources (Welman, Kruger & Mitchel, 2009).

The data gathered and recorded by public service organisations will be a combination of both primary and secondary data whereas the largest chunk of the data will constitute public service sectorial data.

Sectorial data constitutes data that is gathered directly for a specific public service sector such as agriculture, healthcare, civic affairs, environment, tourism and labour. Within an e-Government ecosystem, the main focus will be on utilising and maintaining sectorial data.

Public service organisations may be responsible for one or more administrative sectors as illustrated in Figure 7.2. To distinguish between sectorial data responsibilities, sectorial data can be classified into primary and secondary data domains.

Primary sectorial data constitutes the data that is gathered directly from the source for a specific administration area (i.e., public service sector) by the responsible public service organisation.

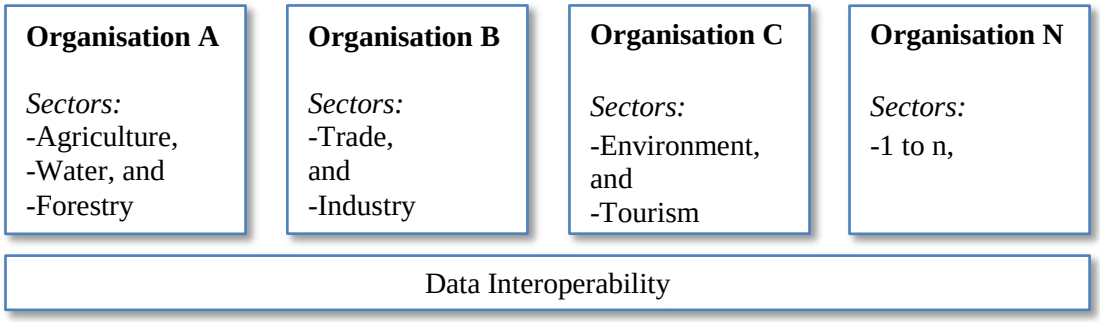

Figure 7.2: Public Service Sectorial Silos

Secondary sectorial data constitutes data gathered by a public service organisation for an administrative area that is not directly under its administrative jurisdiction. The administrative responsibility for the secondary data lies with another public service organisation.

The creation of secondary sectorial data within public service organisations leads to data duplications, data inconsistencies and data quality issues.

To achieve meaningful data interoperability within the public service, the ideal situation will be to substitute secondary sectorial data with primary sectorial data. This could be achieved by sharing and/or exchanging primary sectorial data in a G2G manner.

The adoption of primary sectorial data as a replacement for secondary sectorial data by public service organisations will improve efficiency and decision making, reduce cost and duplications, and increase data credibility.

The volume of primary sectorial data that potentially could be exposed by a public service organisation can be estimated by the following formula:

Exposable Primary Sectorial Data =

Primary Sectorial Data - (Protected Sectorial Data + Constrained Sectorial Data)

7.2.1 Data Value Proposition

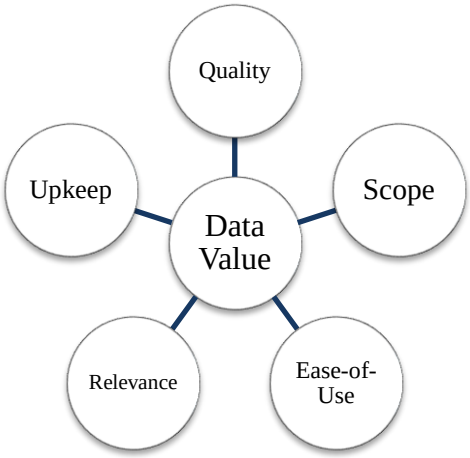

Figure 7.3: Data Value Proposition

The rate of adoption of primary sectorial data within traditional public service delivery environments is mostly low. Low adoption can be explained as a characteristic of the temporary transition from a traditional service delivery mode to a new e-version of service delivery. The reasons for low adoption ranges from inadequate primary sectorial data dissemination from the supply side to poor quality and lack of proficiency in the utilising of data on the demand side.

The demand for primary sectorial data will depend on the relative value (see Figure 7.3) of primary sectorial data to 3rd party public service organisations and stakeholders

(consumers). Five main levels of primary sectorial data demand can be defined as depicted in Table 7.1 for 3rd party consumers. The level of demand will indicate the general need for specific primary sectorial data.

Table 7.1: Levels of Primary Data Demand

Levels	Description
1. No demand	No demand to utilize primary sectorial data.
2. Below Average demand	Very low demand to utilize primary sectorial data.
3. Average demand	Average demand by Government institutions to utilize primary sectorial data.
4. Above Average	More than average demand by Government institutions to utilize primary sectorial data.
5. High demand	Most Government institutions want to utilize primary sectorial data.

The value (i.e., return on investment and benefits) of primary sectorial data to 3rd consumers will be influences by factors such as:

(1) Data Quality: Includes main fundamental characteristics (dimensions) of accuracy, precision, completeness, usability and consistency.

(2) Data Relevance: Data on offer has some bearing or importance applicable to the issue at hand (e.g., process).

(3) Data Scope: The range of a consumer's data needs relevant to the data on offer from the producer of data.

(4) Data Upkeep: The frequency and extent to which data is kept up to date.

(5) Ease of Use: The degree of complexity associated in accessing and using the data.

The value of primary sectorial data can be increased by improving and/or extending the above mentioned data value factors for consumers.

7.2.2 Data Adoption by 3rd Party Consumers

The adoption of primary sectorial data by consumers will be influenced by policy, value of the data, costs involved, external pressures as well as their readiness to utilise the data (see Figure 7.4).

(1) **Law/Policy:** Includes all attributes that lay the enabling foundation for exchanging and sharing primary sectorial data.

(2) **Data Value:** The relative benefit or Return on Investment (ROI) perceived by an entity. Benefits refer to the recognition of the advantages that the data could provide to the organization.

(3) **Costs:** Expenses to be incurred to utilize primary sectorial data.

(4) **External Pressures:** Refers to the persuasive power that external entities exercise on Government institution.

(5) **Readiness:** Consumers ability or level of preparedness to access and utilize primary sectorial data from both organisational as well as a technical perspective.

(6) **Critical Mass:** Refers to the number of public service organisations that are using or planning to use primary sectorial data. According to critical mass theory, an institutions decision to be engaged in a collective action will be dependent on its perception of what the group is doing (Ray, 2009).

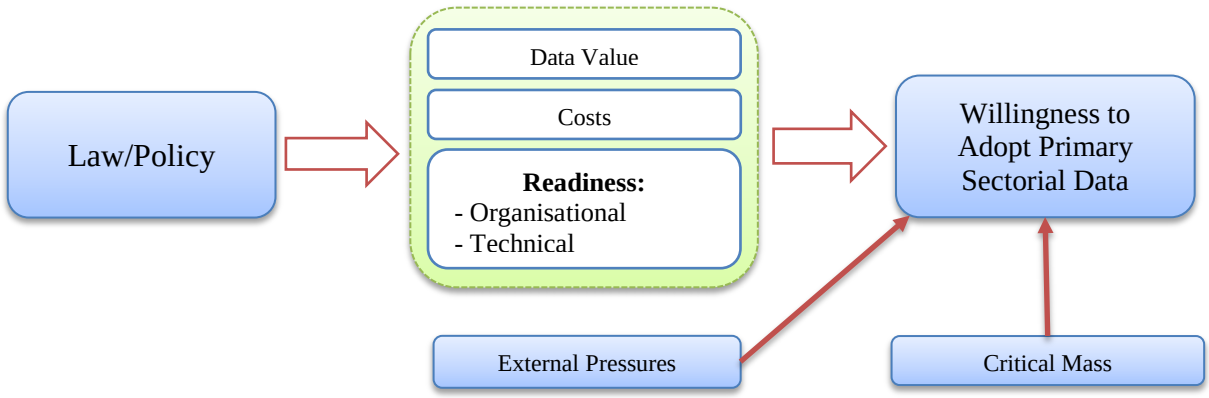

Figure 7.4: Primary Data Adoption Model

The Primary Data Adoption Model illustrated in Figure 7.4 depicts a conceptual model for primary data adoption in an e-Government ecosystem based on seven adoption factor categories.

Table 7.2: Primary Sectorial Data Adoption Rating Template

Categories	Data and Information Policy Provisioning	Data Value	Data Upkeep Frequency	Ease of Use	Organisational Readiness Level	Technical Readiness Level	Critical Mass Influence	Costs Involved	Extent of External Pressures
Ratings									

Rating Scale: 1, 2, 3 where 1 indicates low, 2 indicates medium and 3 indicates high.

Each of the adoption factor categories can be assessed and rated independently using the template of Table 7.2 for each set of primary sectorial data, which collectively provides an indication of a public service organisation's willingness to adopt a given data set.

The willingness aspect of the model will provide a collective map of public service inclinations and preferences towards the adoption of different sets of primary sectorial data.

Based on the demand and data feasibility ratings obtained for each data set, a suitable hierarchical interoperability organisation and solutions can be formulated.

7.2.3 Effect of Supply and Demand on Secondary Sectorial Data

The supply and demand rate of replacing secondary sectorial data within an e-Government ecosystem will follow a similar pattern to the laws of demand and supply utilized within the area of economics as illustrated in Figure 7.5.

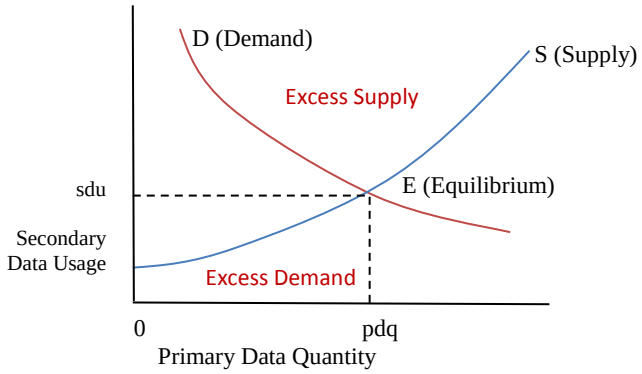

Figure 7.5: Supply and Demand Curve of Primary Sectorial Data

The total amount of primary sectorial data required by public service organisations is referred to as the quantity demanded. The amount of primary sectorial data that a public service organisations offers to consumers is referred to as the quantity supplied.

Prior to meeting the needs of consumers, the level of secondary sectorial data used by public service organisations will be high. As the consumer needs are met for primary sectorial data, the demand and level of usage of secondary sectorial data by public service organisations will decrease.

A demand and supply equilibrium point will be reached when the primary sectorial data offering equals the secondary sectorial data demanded by public service organisations. Supply of primary sectorial data will exceed demand when the supply increases beyond the equilibrium.

The net effect of continuously increasing the supply of primary sectorial data in order to meet demands (see Figure 7.5) will increase data interoperability while at the same time reducing the duplication of data within public service organisations.

7.2.4 Public Service Data Model

At present data within the Public Service is scattered across public service organisations in a multitude of systems as indicated in Section 7.2. To address the planning, decision

making and operational data needs of the public service, sectorial data contained within public service sectors will need to be updated, aggregated, organised and be made accessible to consumers. The conceptual Public Service Data Model as depicted in Figure 7.6 presents a multi-dimensional representation of data within the public service. The Public Service Data Model links sectorial data, data producers and consumers, and data aggregation levels together.

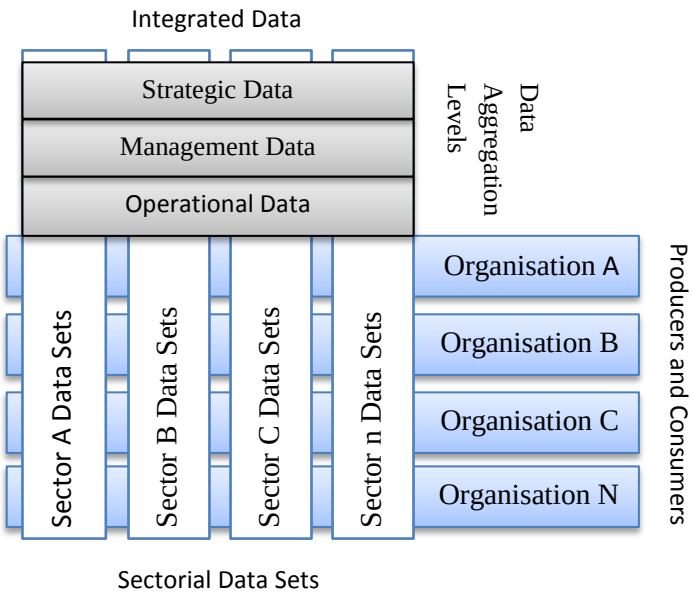

Figure 7.6: Public Service Data Model

From Figure 7.6, different public service organisations produce or require sectorial data sets using different types of systems. The sectorial data sets contained within data silos need to be integrated and exposed at different levels of aggregation to stakeholders. Aggregation of sectorial data requires the integration of the different sectorial data sets contained within the data silos.

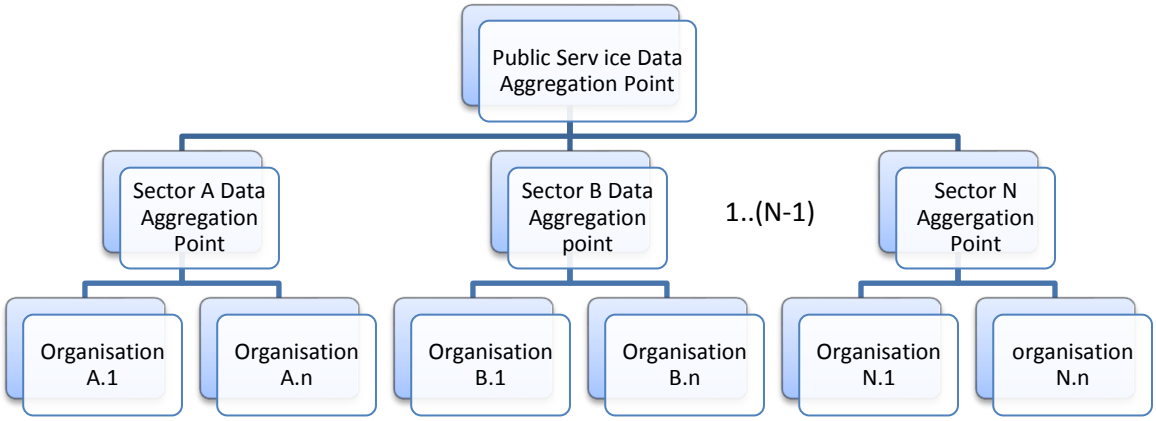

Figure 7.7: Data Aggregation Structure

Data aggregation takes place within organisational and sectorial data silos (vertical aggregation) and across sectorial data silos (horizontal aggregation) at the operational, management and strategic levels. Figure 7.7 illustrates vertical and horizontal data aggregation within the Public Service. The three levels of data aggregation are attended to serve the data needs of the different occupation levels within the public service.

To integrate and expose the sectorial data on the various levels as indicated in Figure 7.7, a Public Service based solution is required. This solution should provide the means to overcome the data interoperability issues of the different sectorial data sets and at the same time address the technical interoperability challenges faced by heterogeneous Information Systems.

7.3 Cooperative Architectural Model (CAM)

The Cooperative Architectural Model (CAM) defines the technical architectural guidelines to establish data sharing and exchange at an organisational, sectorial and public service level.

7.3.1 Design Guidelines

The cooperative architectural design decisions were based on the identified requirements of Section 5.3 and the formulated guiding principles of Section 7.3.1.2. The requirements and principles are summarised in the section below.

7.3.1.1 Requirements

The architectural requirements focus on the non-functional as well as the functional requirements identified by interviewees and related literature studied that should be addressed by the architecture.

The non-functional requirements provide a statement of the expected behaviour of the architecture or constraints placed upon it (Sommerville, 2007). The following non-functional requirements were identified from the interoperability adoption factors identified through the study:

(1) Availability: The architecture should be designed for high-availability by including redundancy.

(2) Integration: Support all required types of integration. Integration covers aspect such as:

- Application connectivity: A connecting (middleware) communications layer which connects the applications interfaces;
- Process integration: Application and services choreography;
- Data and information integration: Store once, use many times.

(3) Maintainability: The architecture should be designed in such a manner as to allow components to be readily changed or updated.

(4) Performance: The Architecture design should localise critical operations within a small number of sub-systems or components. Communication between these sub-

systems or components should be as little as possible. The focus should be on increasing efficiency by reducing processing and communication overhead.

(5) Scalability: Provide the means to remain efficient and effective when there is a significant increase in resource demands or users.

(6) Security: A layered structure should be designed, with the most important resources protected within each layer. The lowest layers should have the highest level of security and the highest layer should have the least security. The layered security structure should ensure that confidentiality, integrity and availability of data is maintained at rest and in transit (Whitman & Mattord, 2003).

The functional requirements provide a statement of the functions or features that should be provided by the architecture (Sommerville, 2007). The following functional requirements were identified by interviewees (see Section 6.3) for interoperability services to be provided by the architecture:

(1) Data Import and Export Services;

(2) Data Replication Services;

(3) File Transfer Services;

(4) RPC Services;

(5) Security Management Services;

(6) Transactional Services; and

(7) Web Services.

7.3.1.2 Design Principles

Architectural design principles define the underlying rules and guidelines for the use and deployment of IT resources and assets across the enterprise (Bachman et al., 2000). These

principals reflect the level of consensus among organisational entities, and form the basis for making IT related decisions in the future.

The guiding principles developed for the architecture were informed by Public Service policies and from the data analysis findings discussed in Chapter 6. The guiding principles defined for the conceptual architecture are the following:

(1) Expose data contained within government organisations and making them more accessible to their consumers.
(2) Safeguard the current IT investments made by interfacing disparate Information Systems without altering them.
(3) Preserve the autonomy of public service organisations.
(4) Reduce the level of data duplication within the Public Service.

The benefits of achieving the above mentioned will be that the Public Service will save costs and effort in their endeavours to establish interoperability within a desperate legacy Information Systems environment.

7.3.2 Conceptual Architecture

The conceptual architecture depicts the conceptual view of the sub-systems (i.e., interoperability hubs) and units as well as the interconnections between them. The high-level conceptual cooperative architecture of CAM is illustrated in Figure 7.8.

The conceptual architecture strives to increase data exchange and data sharing within the Public Service by:

(1) Providing a single point of access for standardised data and services;
(2) Hiding the complexity of the heterogeneous Information System environments from clients;

(3) Reducing infrastructure duplication by using common infrastructure and services; and

(4) Providing an effective approach to integrate legacy Information Systems.

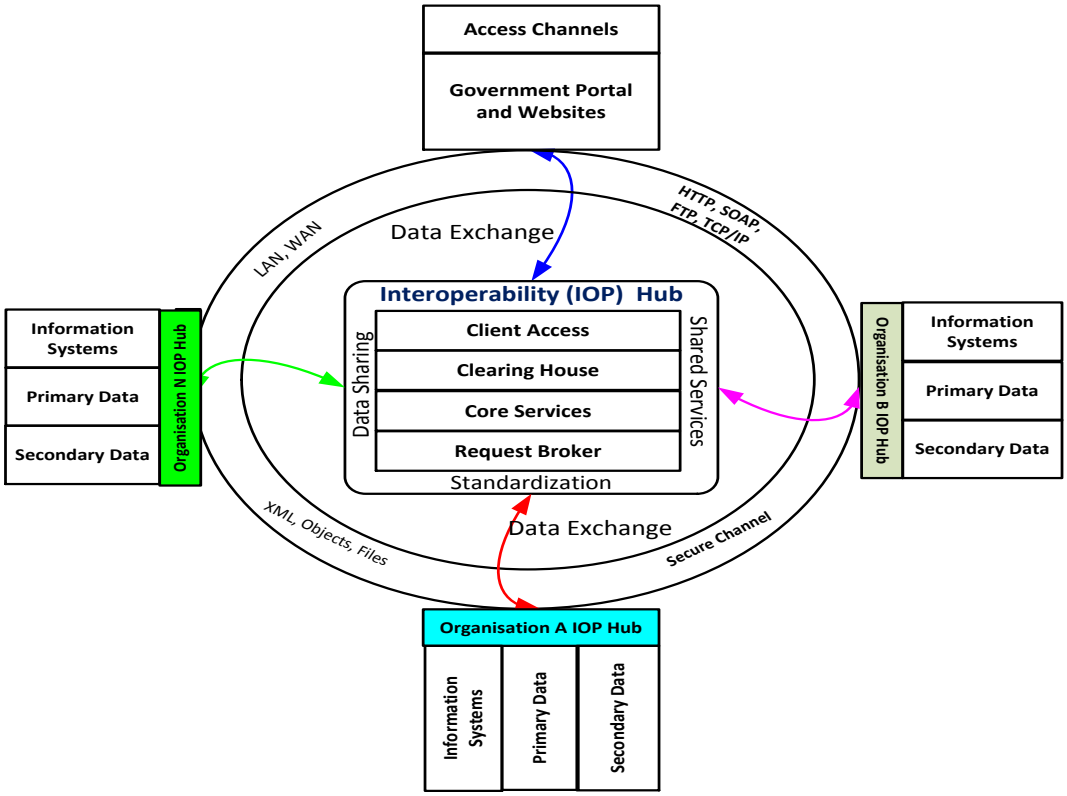

Figure 7.8: Conceptual Cooperative Architecture Model (CAM)

The conceptual architecture as illustrated in Figure 7.8 focuses on both vertical and horizontal interoperability within the Public Service. Vertical interoperability addresses the sharing and exchanges of data within a public service organisation whereas horizontal interoperability focusses on inter organisational data sharing and data exchange. The conceptual architecture further extents interoperability to the e-Government level by exposing data contained within different organisations to the Government Portal and its websites.

The conceptual CAM as depicted in Figure 7.8 consists of central and organisational interoperability hubs which are connected by shared communication networks (e.g., LAN, WAN).

Interoperability hubs are sub-systems of a hosting platform. The sub-systems are composed of units with defined application interfaces. The unit interfaces are used to communicate with other units through their public and protected application interfaces. The units provide the means to obtain and transform data gathered from various heterogeneous Information Systems. The data transformed by units are finally presented as one consolidated data stream to data consumers (e.g., Information Systems, interoperability hubs) through their application interfaces.

The different units of an interoperability hub are depicted in the central interoperability hub of Figure 7.8. The central interoperability hub is responsible to expose, share and exchange data with the Government Portal, websites and organisations (i.e., horizontal interoperability) through the central or organisational interoperability hubs. Organisational interoperability hubs provide the means to broker and share data within an organisation.

The central and organisational interoperability hubs are of similar design, forming an edge and federated collaborative distributed system. This collaborative configuration will allow interoperability hubs to:

(1) Provide data services to data consumers;
(2) Redirect requests to other Information Systems and interoperability hubs;
(3) Manage the aggregation and replication of data; and
(4) Broker data between different heterogeneous Information Systems and interoperability hubs.

The different organisational and gateway based interoperability hubs are connected to the central interoperability hub by LAN or WAN connections through a secured and reliable communication channel (e.g., SSL, TLS). Requests and responses are transmitted in the form of XML documents (SOAP messages), objects (RPC calls) or files (File transfers) between the interoperability hubs using the HTTP, HTTPS, SOAP, FTP, SFTP or RMI-IIOP protocols. Communication between interoperability hubs may be synchronous or asynchronous in nature.

The CAM as presented in Figure 7.8 represents a foundation model for establishing interoperability within the Public Service. The configuration of Figure 7.8 can be scaled upwards to improve accessibility, security and performance. This can be achieved by increasing the number of interoperability hubs at the centre of the configuration of Figure 7.8. These interoperability hubs could then be loosely coupled to collectively form a central cooperative service bus to which organisational interoperability hubs can connect. The cooperative service bus will conceptually form an enhanced central interoperability hub.

The CAM's interoperability hub structure and logical organisation is decomposed and described in more detail in the Sections 7.3.2.1 and 7.3.2.2 respectively.

7.3.2.1 Interoperability Hub Layered Architecture

The layered architecture view of the central interoperability hub depicted in Figure 7.8 is detailed in Figure 7.9. The layered interoperability hub architectural view was documented using the guidelines and notions of Bachman et al. (2000).

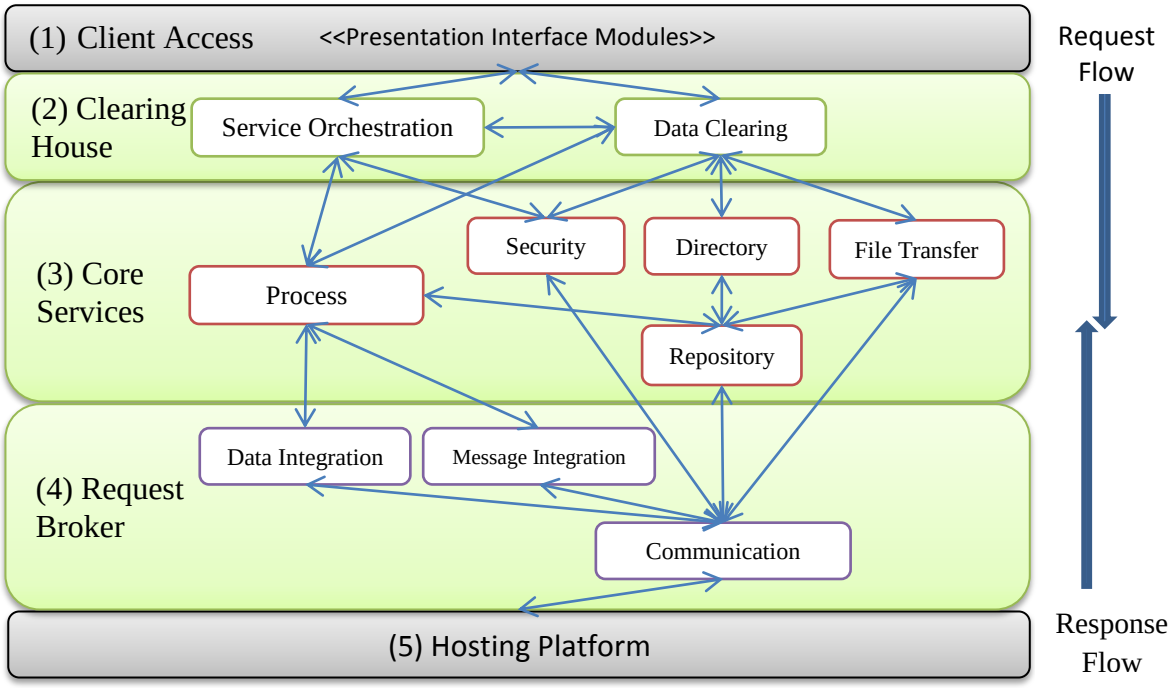

Figure 7.9: Interoperability Hub Layered Architecture

Figure 7.9 uses the stack paradigm to represent the layered interoperability hub architecture. In this type of notation, layers are indicated as a stack of rectangles. The relation between layers is denoted by geometric adjacency. The horizontal edges between rectangles denote the interfaces to the layer.

The layered view of Figure 7.9 reflects a division of the software into units (e.g., programs and modules), with each unit forming a layer. The layers serve to partition the software, with each partition forming a virtual machine that provides a cohesive set of services through interfaces. Layers interact with each other in an ordered relation whereby the relation between layers indicates what programs or modules may be used between them.

Inter-layer usage only occurs via interface facilities provided by programs or modules within a layer.

Requests flow down the layered stack while responses flow up the layered stack. The entry point for client requests into the layered stack is through the Client Access layer (see Figure 7.9). Responses may be generated at any layer of the stack, which will be returned to the requester.

The different layers (i.e., units) and modules of the interoperability hub architecture of Figure 7.9 are described below:

(1) Client Access: This layer serves as the point of entry for service consumers (i.e., clients). The Client Access layer is responsible for the communication with clients through standardised presentation interfaces. Different communication access channels are serviced through this layer. The presentation interfaces will provide clients with common interfaces that they can use to find data and services on offer, subscribe to data or share data. Request made through any of the presentation interfaces will be forwarded to the Clearing House layer for further action.

(2) Clearing House: The Clearing House layer serves as the business logic layer of the architecture and is primarily responsible for service orchestration and data clearing. The modules provided in this layer will interact with the modules within the Clearing House and Core Services layer.

- **Service Orchestration:**

  The role of the Service Orchestrator module is to define and execute business processes whose configuration and flows are determined by business and process logic. The Service Orchestration module will be responsible to coordinate and direct service requests made through the Client Access layer.

This module will make use of workflow patterns in executing service requests. The workflow patterns will define the different data exchange scenarios and indicate the sequence of the services to be executed for each scenario. The Service Orchestrator module provides the capability to define and update workflow patterns for each of the different data exchange scenarios.

- **Data Clearing:** The Data Clearing module is responsible to manage the publishing and subscriptions to available data sets. The subscription services offered by the Data Clearing module will allow users to subscribe to standardised publications of primary sectorial data sets offered. In addition, the Data Clearing module will provide the mechanisms to submit data, categorise, grade and clear shared data sets for publishing. A high level lookup service is provided in this module to locate publications of data sets and services offered by this layer.

(3) Core Services: The Core Services layer consists of five loosely coupled modules that provide core services through their public and protected interfaces to the modules of the adjacent architectural layer in the areas of security, data sharing, data exchange and repository services. The following core modules are located within this layer:

- **Process Services:** The Process Services module provides the mechanism to look-up and instantiate published services stored within the services repository. The module is further responsible for the deployment, un-deployment and monitoring of published services.
- **Directory Services:** The Directory Service module is used to create a descriptive catalogue of all published services and data. The directory repository maintains consumer subscription information as well as data

provider information. In addition, the Directory Service module provides catalogue update and query services.

- **File Transfer Services:** This module is responsible to facilitating the transfer of structured (e.g., Fixed column text files, CSV files) and unstructured (e.g., PDF Files, Word Documents) files between hosts and consumer systems.
- **Repository Services:** The Repository module provides the mechanism to store published services and share data. The module also provides data replication and resource update services to add, edit or delete data or services from the repository.
- **Security Services:** Provides the security related services to support the interoperability hub architecture in the areas of authentication, authorization, auditing and encryption. The Security Service module provides functionalities to register users and to assign user access rights to the shared resources provided by the interoperability hub.

(4) Request Broker: The Request Broker layer acts as a single point of data and message transformation and integration for both service consumers and producers. The transformation principal for this layer is illustrated in Figure 7.10.

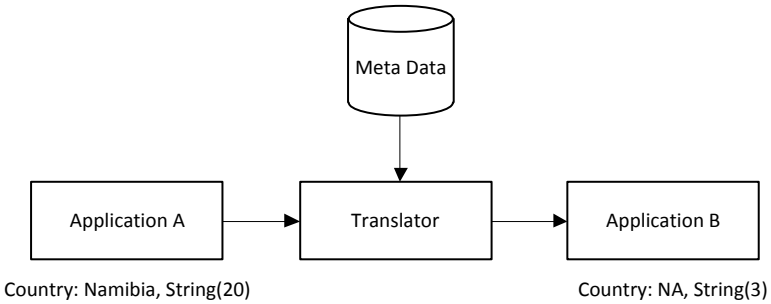

Figure 7.10: Syntactic and Semantic Data and Message Transformation

The layer further is responsible for managing communication between databases and compliant applications and enterprise middleware systems. Both synchronous and asynchronous communications is supported through this layer.

- **Data Integration:** The Data Integration module provides the functionalities to transform data structures (meta-data) from a producer system to standard data structures that can be consumed by consumer systems. Additionally it will provide mechanisms to transform the data exchanged between different data domains to a standard semantic format that can be used by consumer systems. Based on the data requirements, the module can merge or partition data required by consumers. Native adopters are used by this module to connect to database and application systems.
- **Message Integration:** The Message Processing module acts as a single point of message transformation, aggregation and forwarding for both service consumers and producers. The module provides the means to connect to compliant applications and enterprise middleware systems through different messaging mechanisms.
- **Communication**: This module is responsible to establish and managing communication between systems. The Communication module's functions include the establishing and managing of connections, routing, addressing, queuing and protocol conversions.

(5) Hosting Platform: The platform provides the hosting and supporting application environment on which the interoperability hub will run.

The layered architecture presented may be implemented using component based and service oriented technologies from commercial software development companies or from open source initiatives.

7.3.2.2 Distribution Architecture

The CAM interoperability hub organisation concept (see Section 7.3.2) is further detailed in the Distribution Architecture. The Distribution Architecture shows how interoperability hubs may be organised and distributed across the Public Service to facilitate the sharing and exchange of data. The interoperability hub as described in Sections 7.3.2.1 may be deployed in the following ways:

(1) Cooperative Client-Server Architecture: In this model, the server is deployed as a central interoperability hub between client systems. All services are centralised within a single interoperability hub server. Clients directly connect to the server to request or receive data.

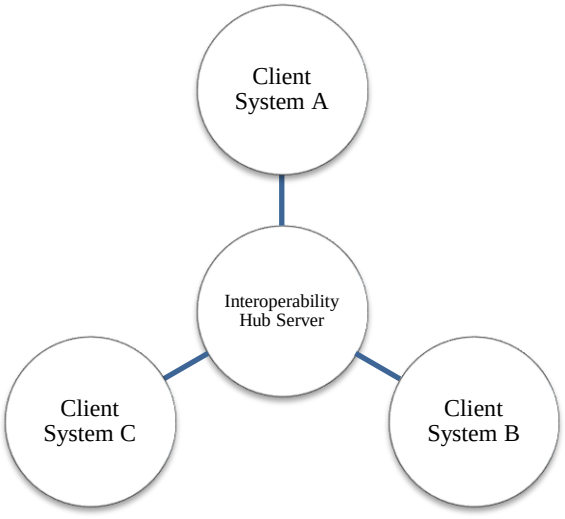

Figure 7.11: Cooperative Client-Server Architecture

Figure 7.11 depicts the Cooperative Client-Server Architecture in a hub-and-spoke configuration. In this type of architecture, all data exchanges requests are made by clients to the central interoperability hub. The central interoperability hub provides

a broad range of interoperability services which will obtain and format data on behalf of clients. The formatted data will be returned to clients by the central interoperability hub as responses to their requests. Other interoperability hubs can be connected to the central interoperability hub as clients.

(2) **Cooperative Service Bus Architecture:** In this model, interoperability hubs are deployed as a set of distributed interoperability hubs to form a Cooperative Service Bus for a specific service domain. Services provided are spread across interoperability hubs, with each interoperability hub being responsible for a specific set of services. Services offered by interoperability hubs will be exposed to clients as publications. Clients within the same service domain will be allowed to subscribe to the published services.

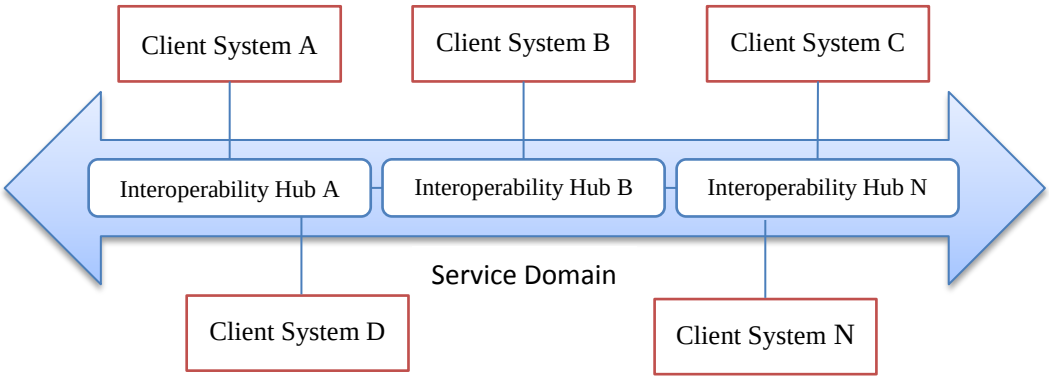

Figure 7.12: Cooperative Service Bus Architecture

From Figure 7.12, interoperability hubs are interconnected to form a single loosely coupled interoperability service domain. Each of the interoperability hubs will offer a range of interoperability services for specific service domains. Clients connect to a selected interoperability hub that fall within their service domain. Services not found within a specific interoperability hub will be negotiated and brokered with the relevant interoperability hub within the service bus. The Cooperative Service Bus Architecture will allow public service organisations within different sectors to

connect, mediate, and control the interaction across the highly distributed and heterogeneous environments of the Public Service.

The two distribution architectures explained above may be combined to form the Public Service Cooperative Distribution Architecture that models the interoperability hub organisations of conceptual CAM (see Section 7.3.2) and the Public Service Data Model of Section 7.2.4. The combined hybrid Distribution Architecture is depicted in Figure 7.13.

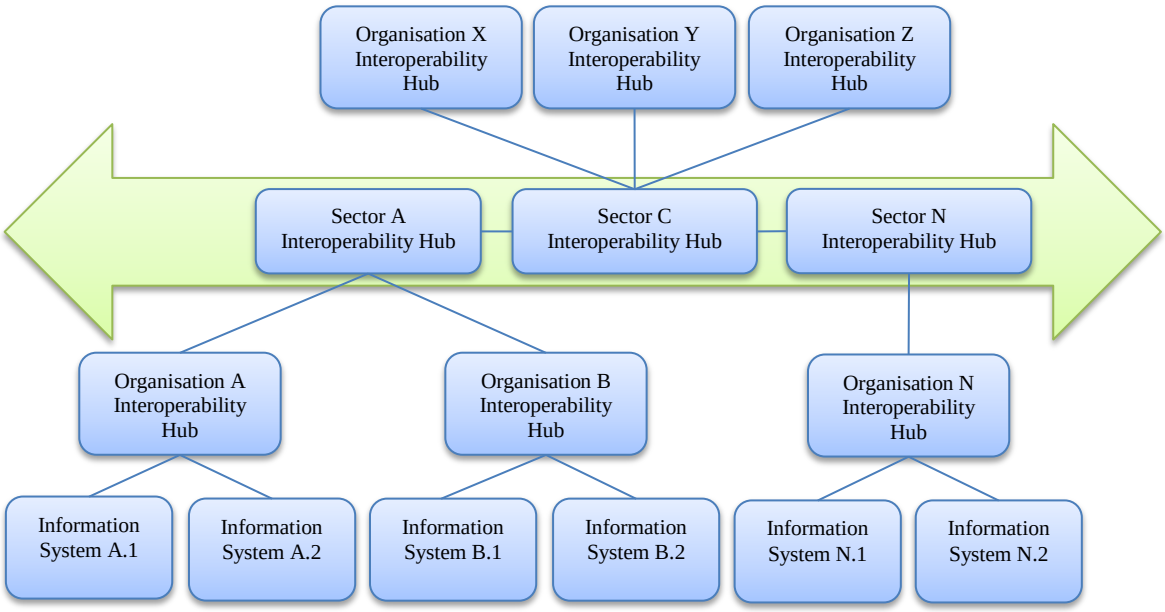

Figure 7.13: Cooperative Deployment Architecture

The Cooperative Distribution Architecture interoperability hub organisation for the Public Service of Namibia is presented in Figure 7.13. The Cooperative Distribution Architecture connects different public service sectors and organisations together to facilitate the sharing and exchange of data within the heterogeneous environment of the Public Service. The deployment architecture addresses both vertical and horizontal interoperability. Vertical interoperability is at the organisational and sectorial levels whereas horizontal interoperability is at a public service level.

(1) **Vertical Interoperability:** At the organisational level, a central organisational interoperability hub is used to share and exchange information with Information Systems of that organisation. The organisational interoperability hub intern is connected to a sectorial interoperability hub. Sectorial interoperability hubs provide the means to share and exchange information between organisations which share the same public service sector. The system organisation between Information Systems, organisational interoperability hubs and sectorial interoperability hubs is of the Interoperability Client-Server Architectural form.

(2) **Horizontal Interoperability:** Horizontal interoperability is established by connecting interoperability hubs at the sectorial level together to facilitate the sharing and exchange of data among different public service sectors. The sectorial hubs are configured as a Cooperative Service Bus Architecture that spans all public sectors.

The proposed Cooperative Distributed Architecture can be further extended to the public realm (e.g., G2C, G2B) by connecting the Government Portal and websites to the Public Service Cooperative Service Bus. In this configuration, portal services will be able to interact with services of the Cooperative Service Bus to obtain standardised, categorised and graded data which could be further processed and presented to portal service consumers.

7.3.3 Validation and Review of Theoretical Models

The content of this chapter was reviewed by the OPM e-Government technical expert group as well as by external international reviewers.

7.3.4 Internal Validation within the Public Service

The conceptual CAM and its software architectural views were validated against the architectural requirements, principles and typical interoperability scenarios found within the public service environment. The different scenarios that were tested against the theoretical models are listed below:

(1) Establish data sharing and exchange between two or more legacy Information Systems within a public service organisation;
(2) Facilitate data sharing and exchange between two public service organisations; and
(3) Facilitate data sharing and exchange between the public service and external stake holders.

The validation of the CAM was performed by the e-Government expert group in the OPM a structured walkthrough process as described in section 3.2.4.

The feedback obtained from the expert group during the structured walkthrough process was incorporated into the CAM. The updated CAM was submitted for final review to the OPM e-Government expert group where it was accepted and signed-off.

7.3.5 External Review

Sections 7.2 and 7.3 of this chapter, which includes the conceptual CAM, was abstracted and submitted as a conference paper entitled “The Analogy of Data within eGovernment Interoperable Ecosystem (AD-eGIE): Utilising Sectorial Information” to IST Africa for the IST Africa conference of 2011 in Gaborone, Botswana. The paper was peer reviewed and accepted into the conference proceedings. In September 2011, permission was requested and granted to IST Africa to submit the paper to IEEE-XPlore for publishing in their journal.

7.4 Summary

The chapter provided an analogy of data within the public service and proposed a data model based on the findings. The data model developed consists of multiple dimensions that focus on the organisational, sectorial and data abstraction levels of the public service. The data model together with the data analysis findings formed the basis for the architectures and models developed and discussed in this chapter.

The conceptual Cooperative Interoperability Architecture (CAM) is proposed in this chapter. The CAM serves as an architectural blueprint to establish interoperability within the Public Service of Namibia. The CAM consists of interoperability hubs that facilitate data sharing and exchange at different levels of the Public Service. The deployment of interoperability hubs at the organisational and sectorial levels follows the well-known Client-Server Architectural model whereas at the Public Service level a Cooperative Service Bus Architecture was devised and utilised. The Distribution Architecture of the CAM provides a flexible structure that could be deployed in any number of configurations.

The CAM architecture presented incorporates the majority of the requirements and suggestions made by the international and OPM e-Government experts.

8. CONCLUSION AND FUTURE RESEARCH

In this chapter, the summary of the conclusions on the research questions will be presented for each of the research questions posed. The chapter concludes with a study achievements summary and suggestions for future research.

8.1 Introduction

The research conducted focussed on the current and required state of technical interoperability within the Public Service of Namibia. The research also investigated the factors that may influence the adoption of interoperability by the Public Service of Namibia. This chapter presents the main findings of the research, summary of the study achievements and provides some suggestions for future research.

8.2 Conclusion

The conclusions are discussed in relationship to the research questions. The research questions guided the research and data analysis.

8.2.1 Research Question One: "Which forms of technical interoperability exist within the Public Service of Namibia?"

Based on the discussion of Chapter 6, Section 6.2 of this thesis, technical interoperability was established on the Interoperability Coalition Model (see Section 4.3) layers of data, software, communication and physical interoperability by public service organisations. The overall level of technical interoperability attained by the Public Service was at a fairly low level ('Ad-hoc' level) of technical maturity at the time of the investigation. In particular, technical interoperability maturity was attained as follows on the different interoperability layers as defined:

(1) **Data Interoperability:** Interoperability of data between Information Systems was attained at Level 1 ('Manual' level), which is the lowest level of data interoperability maturity. Data between Information Systems were mostly exchanged through file transfers, data import-export and transactional services. Data exchanges were mostly done manually between Information Systems.

(2) **Software Interoperability:** Software interoperability was attained at Level 2 ('Ad-hoc' level) of software interoperability maturity. The Public Service utilised a wide variety of software for their Information Systems. A limited number of the Information Systems pairs that exchange data have to some degree solved the software compliancy differences between them.

(3) **Communication Interoperability:** Communication between Information Systems was attained at Level 2 ('Ad-hoc' level) of communication interoperability maturity. Information Systems mostly utilised the same communication protocol, however very few interfaces were provided by Information Systems that would allow communication and interaction between them.

(4) **Physical Interoperability:** Physical interoperability was attained at Level 2 ('Ad-hoc' level) of physical interoperability maturity. A small number of Information Systems made use of a shared communication network to exchange data. Most of the Information Systems were isolated within the private networks of public service organisations with limited means to connect to external systems.

Technical interoperability between Information Systems was achieved by creating unique tightly coupled data exchange mechanism for each pair of interoperating Information Systems. Electronic data exchanges between Information Systems were performed as file transfers or as database transactions through a Client-Server type systems architecture arrangement. Data exchanges between Information Systems were based on multitude of

localised unique standards. At present no overarching Public Service interoperability standards exist.

In conclusion, the research indicated that technical interoperability was established on all technical interoperability layers at different levels of sophistication. Overall technical interoperability within the public service was at a low level. The low level of existing interoperable Information Systems and heterogeneous interoperability landscape provides a very fragile foundation for any e-Government initiative to be undertaken.

8.2.2 Research Question Two: "What forms of models will be required to establish technical interoperability within the Public Service of Namibia?"

The discussion of the data analysis (see Chapter 6) indicates that there is need to become more technical interoperable. The findings suggest that the number of interconnections between Information Systems within the Public Service should be expanded and that the level of interoperability sophistication and compliancy be increased. Through the data analysis, the need identified was to increase the overall technical interoperability maturity level of Information Systems environments from an 'Ad-hoc' level to an 'Integrated' level.

At an architectural level, the data analysis findings identified three different types of systems architectures desired by interviews to share and exchange data, namely: (1) Client-Server Architecture, (2) Service Oriented Architecture and (3) Peer-to-Peer Architecture. A number of requirements were identified by interviewees for the desired interoperability architecture. The requirements are summarized in Table 6.2 of Chapter 6 as well as in Section 7.3.1.1 of Chapter 7.

In conclusion, the public service requires a standardized hybrid interoperability architecture that will allow heterogeneous Information Systems to share and exchange data at an 'Integrated' level of sophistication and compliance.

8.2.3 Research Question Three: "What factors will influence the adoption of interoperability within the Public Service of Namibia?"

The public service is increasingly becoming aware of the need to become more interoperable within and between public service organisations. From the data analysis discussion of Chapter 6, there is a need to move the Public Service to a higher level of interoperability that will provide the basis for e-Government. The transition from the current state to the desired state of interoperability (see Figure 7.1) will be influenced by a number of interoperability adoption factors.

Based on the discussion under Section 6.4 of Chapter 6, 24 distinct interoperability factors where identified. The seven most identified factors found through the analysis were that of (1) 'Data Security', (2) 'Data quality', (3) 'Connectivity', (4) 'Compatibility', (5) 'Performance', (6) 'Infrastructure Security' and (7) 'Accountability'.

Three notable statistical significant correlations where also found between the seven most identified interoperability adoption factor variables. The correlations identified suggest that:

(1) 'Data Security' plays a major role in the 'Connectivity' of Information Systems;

(2) 'Accountability' plays a role in 'Data Quality'; and that

(3) 'Compatibility' plays a role in the form of 'Infrastructure Security' established.

In conclusion, the above mentioned interoperability adoption factors pose a considerable risk to the establishing of interoperability within the Public Service. These adoption factors

will need to be addressed during the technical interoperability solution design phase so as to increase the willingness of public service organisations to adopt interoperability solutions and to participate in the sharing and exchange of data.

8.2.4 Proposed Conceptual Architecture Model

Based on the requirements identified through the interview process, supporting models (e.g., ISIMM, Public Service Data Model) were developed and the architectural design principles defined (see Section 7.3.1.2), the Cooperative Architectural Model (CAM) was proposed in Chapter 7 as an architectural blueprint to facilitate the sharing and exchange of data within the Public Service in a standardised manner. The CAM design proposes that data sharing and exchange be coordinated through standardised interoperability hubs that serve as middleware between different types of Information Systems. The interoperability hubs of the CAM can be organised in any number of architectural configurations. Section 7.3.2.2 proposes that interoperability hubs be organised in a Cooperative Client-Server type configuration at organisational and sectorial levels, and as a Cooperative Service Bus at the level of the public service. This type of architectural arrangement provides an efficient and economical way of sharing and exchanging data within a heterogeneous Information Systems environment while providing the Public Service with the means to move to an advanced level of data and service integration.

In conclusion, the CAM proposed in this study meets the architectural requirements and serves as a conceptual blueprint for achieving the desired state of technical interoperability. The implementation of CAM should be guided by the GIGF and its associated implementation process cycle (see Section 4.3). The ISIMM could serve as a measure to establish the level of compliance and sophistication obtained of the CAM implementation.

8.3 Summary of Achievements in this Study

This study has achieved what it set out to accomplish by providing a public service centred Cooperative Architectural Model (CAM) in Chapter 7 that can be used to guide the establishing of technical interoperability within the context of the Public Service of Namibia.

In defining the architecture, three core areas of concern were studied which focused on the current state of interoperability, required state of interoperability and interoperability adoption factors. The analysis findings (see Chapter 5) and discussion (Chapter 6) provided insight into the forms and levels of technical interoperability attained and required by the Public Service of Namibia. The study of the current and required state of interoperability indicated that there was need to advance interoperability to a higher level of sophistication and compliance within the Public Service. Further insight was also provided into the factors that may influence the adoption of interoperability at an organisational as well as at a technical level.

The study in addition to CAM offers six models and one framework that provide additional guidance and benchmarking to establish interoperability within the Public Service, namely:

(1) **ISIMM:** A model and matrix to assess the degree of sophistication and compliance between Information Systems (see Section 3.5.4).
(2) **GIGM and GIGF:** The model and framework serves as an overall governance guide in the development of Government Interoperability in areas of policy, people, procedures and technology (see Chapter 4).
(3) **Interoperability Coalition Model:** This model identifies, demarcates and defines the different interoperability layers in a rank ordered stack (see Section 4.3).

(4) **Conceptual Model for Interoperability Adoption within the Public Service Environment:** The model depicts the interoperability adoption factor domains and the relationships between them that will individually as well as collectively influence the establishing of interoperability within the Public Service (see Section 6.4).

(5) **Primary Data Adoption Model:** A conceptual model for primary data adoption in an e-Government ecosystem (see Section 7.2.2).

(6) **Public Service Data Model:** A multi-dimensional conceptual model that provides a representation of data within the Public Service (see Section 7.2.4).

It is anticipated that the framework and models suggested in this thesis will provide the conceptual basis for the interoperability initiative as defined under the Public Service e-Government Plan of Action of 2011.

8.4 Future Research

The study conducted primarily focussed on the technical aspects of interoperability with the aim to create a public service centred Cooperative Architectural Model (CAM) that would define and guide the establishing of technical interoperability within the context of the Public Service of Namibia.

The technical interoperability study performed can be extended in the future to the domain of organisational interoperability. The organisational interoperability study can for example look at interoperability of business goals, business processes and data architectures within the Public Service.

The study was narrowly focussed on the Public Service of Namibia; this study could be extended to the local and regional government levels. Such a study could focus on interoperability between central, regional and local governments within Namibia.

An important extension of this study will be to implement and test the conceptual CAM within a heterogeneous Information Systems environment. Such a study could focus on the technology architecture that would be required to realise the CAM. The non-functional requirements as defined in section 7.3.1.1 could serve as a benchmark for the technology solution.

From interoperability solution implementation viewpoint, it is interesting to study the factors that may impact the implementation.

REFERENCES

Bachman, F., Bass, L., Carriere, J., Clements, P., Garlan, D., et al. (2000). *Software Architecture Documentation in Practice: Documenting Architectural Layers.* (Special Report CMU/SEI-2000-SR-004). Carnegie Mellon: Software Engineering Institute.

C4ISR Architectural Working Group. (1998). *Levels of Information Systems Interoperability (LISI).* Retrieved March 7, 2011, from http://www.defencelink.mil/nii/org/cio/i3/lisirpt.pdf

Clark, T. & Jones, R. (1999). *Organisational Interoperability Maturity Model for C2.*, Command and Control Research and Technology Symposium. Retrieved March 7, 2011, from http://www.dodccrp.org/events/1999_CCRTS/pdf_files/track_5/049clark.pdf

Coulouris, G., Dollimore, J. & Kindberg, T. (2009). *Distributed Systems Concepts and Design* (4th ed.). Harlow, England: Addison-Wesley.

Fan, J. & Zhang, P. (2007). *A Conceptual Model for G2G Data Sharing in E-Government Environment.* The Sixth Wuhan International Conference on E-business. Wuhan, China.

Government of the Republic of Namibia. (2011). *National eGovernment Strategic Action Plan: eGovernment Readiness Report.* Windhoek, Namibia: Author.

IDABC. (2004). *European Interoperability Framework for Pan-European e-Government Services (EIF)* (Ver. 1). Luxemburg: European Communities.

Jolma, A. & Rizzoli, A. (2003). *A Review of Interoperability Techniques for Models, Data, and Knowledge in Environmental Software.* International Congress on Modelling and Simulation. Retrieved September 4, 2011, from http://www.mssanz.org.au/MODSIM03/Volume_04/C05/06_Jolma.pdf

Kamal, M. K., Themistocleous, M. & Elliman, E. (2008). *Mapping Factors Influencing EAI Adoption in the Local Government Authorities on Different Phases of the Adoption Lifecycle.* European and Mediterranean Conference on Information Systems (EMCIS2008). Retrieved November 2, 2011, from http://bura.brunel.ac.uk/bitstream/2438/4016/1/C58.pdf

Lallana, E.C. (2008). *E-Government Interoperability.* Bangkok: United Nations Development Programme.

Ministry of Finance and Deregulation. (2005). *Australian Government Technical Interoperability Framework.* Australia: Author.

Ministry of Information and Communication Technology. (2009). *Overarching ICT Policy for the Republic of Namibia*. Windhoek, Namibia: Author.

Ministry of Information and Communication Technology. (2008). *IT Policy for the Republic of Namibia*. Windhoek, Namibia: Author.

Namibia Public Service Committee on IT Technology. (2004). *IT Technology Policy for the Public Service (Vol. 3).* Windhoek, Namibia: Author.

Office of the President. (2008). *Third National Development Plan (NDP 3) 2007/2008 – 2011/12* (Vol. 2). Windhoek, Namibia: Author.

Office of the Prime Minister. (2004). *E-Governance Awareness: Serving You Online.* Windhoek, Namibia: Author.

Office of the Prime Minister. (2005). *E-Governance Policy for the Public Service of Namibia*. Windhoek, Namibia: Author.

Pankowska, M. (2008). National Frameworks' Survey on Standardization of E-Government Documents and Processes and Processes for Interoperability. *Journal of Theoretical and Applied Electronic Commerce Research,* 3(3). Retrieved November 2, 2011, from http://redalyc.uaemex.mx/pdf/965/96530306.pdf

Pardo, A. & Burke, G.B. (2008). *Improving Government Interoperability: A Capability Framework for Government Managers.* Retrieved September 10, 2010, from University at Albany, Center for Technology in government Web site: http://www.ctg.albany.edu/publications/reports/improving_government_interoperability

Ray, D. (2009). Adoption of Interoperability e-Government Systems: A Research Perspective. *Thought Avenue.* Retrieved September 3, 2010, from http://www.thougthavenue.com/Articles/2.pdf

Sanchez, A., Janowski, T., & Estevez, E. (2008). *Interoperability for E-Government: Technical Report* (Ver. 1), United Nations University, Center for Electronic Governance.

Sarantis, S., Charalabidis, Y., & Psarras,J. (2008, May). Towards Standardising Interoperability Levels for Information Systems of Public Administration. *Electronic Journal for e-Commerce Tools and Applications (eJETA),* Retrieved November 2, 2011, from http://www.ejeta.org/specialMay08-issue/ejeta-special-08may-5.pdf

Satzinger, J.W., Jackson, R.B., & Burd, S.D. (2002). *Systems Analysis and Design in a Changing World* (2nd ed). Boston: Thomson Learning.

Schimdt, J.G. & Lyle, D. (2010). *Lean Integration: An Integration Factory Approach to Business Agility.* Boston: Addison-Wesley.

Sommerville, I. (2007). *Software Engineering* (8th ed.). Harlow, England: Addison-Wesley.

State Services Commission. (2006). *Enabling Transformation: A Strategy for e-Government.* Wellington: New Zealand.

Tanenbaum, A.T., & Van Steen, M. (2007). *Distributed Systems Principles and Paradigms* (2nd ed). New Jersey: Pearson Prentice Hall.

United Nations Department for Economic and Social Affairs. (2008). *United Nations E-Government Survey 2008: From E-Government to Connected Governance.* New York: United Nations.

United Nations Educational, Scientific and Cultural Organization. (2005). *E-Government Toolkit for Developing Countries.* New Delhi: United Nations.

United Nations Development Programme. (2007). *E-Government Interoperability: Guide.* Bangkok: United Nations.

U.S. Department of Energy. (2002, September). *System Engineering Methodology: Structured Walkthrough Process Guide* (Ver. 3). United States: Author.

Welman, Kruger & Mitchel. (2009). *Research Methodology* (3de ed.). Cape Town: Oxford Press.

Whitman, M.E., Mattord, H.J. (2003). *Principles of Information Security*. Canada: Thomson.

APPENDIX A –INTERVIEW GUIDE

The interview sessions were guided by the interview guide. The interview guide consists of different sections which contain leading and guiding questions relating to the different aspects of the study. These questions were partially used during the interview sessions to initiate and further the interview discussions. Therefore, not all discussed subjects are covered by the questions as listed in this appendix. The interview guide and its different sections are detailed below.

Technical Interoperability Interview Guide

The objective of the interview is to establish the current state of technical interoperability, required state of technical interoperability and the adoption factors that will influence the adoption of technical interoperability by a public service organization.

Section 1 – General

Establish which Information Systems are available within the organization and if interoperability is taking place.

- Which Information Systems are at present operational within your organisation?
- Which of these Information System(s) are exchanging data or information?

Section 2 - Current State of Interoperability

Questions focused on determining the form of interoperability used by Information Systems by looking at the collaboration, standards, data as well as infrastructure aspects of interoperability.

2.1 Standards

Guiding questions directed at identifying existing technical interoperability references and compatibility standards.

- Which interoperability reference or compatibility standards have your organization developed or adopted?

2.2 Collaboration

Guiding questions directed at establishing which organizations are exchanging data, process domains involved and the nature of exchange.

- Which sets of organizations/entities are exchanging data?
- In what manner is data being exchanged? (manually or electronically)

2.3 Data and Information

Guiding questions focused on establishing the data domains, structure and the form of data being exchanged.

- Are any of the data shared with other organisations?
- In what format is the data presented or provided to other organisations?
- Are meta-content about available data made available to other organisations?
- Are common definitions (data model) provided for shared data?
- How are data secured and protected?

2.4 Infrastructure

Guiding questions focused on describing the interoperability technology infrastructure utilized by the organization.

- What form of n-tier interoperability architecture is employed to exchange or share data?

- What form of electronic services is provided for sharing or exchanging data?
- Which communication high-level protocol(s) are used to exchange data among interoperable systems?
- Which network form is utilized to establish communication between the interoperable systems?

Section 3 - Required State of Interoperability

Questions focused on determining the form of interoperability required by organizations within the next three years based on their interoperability needs. Aspects such as collaboration, standards, data and infrastructure interoperability will be focused on.

3.1 Collaboration

Guiding questions directed at establishing the organizations that would like to exchange data and the form of interaction required.

- With which organizations/entities will the organisation like to share or exchange data?
- Which information systems would most likely be involved?

3.2 Standards

Guiding questions concerned with technical interoperability referenced or compatibility standards required by an organization.

- Is your organisation planning to develop or adopt any data interoperability reference or compatibility standards for the form of interoperability required?
- Is your organisation planning to develop or adopt any infrastructure interoperability reference or compatibility standards for the form of interoperability required?

3.3 Data and Information

Guiding questions focused on establishing the form and class of data required or offered by an organisation?

- What data presentation form is preferred for data interchange?
- What form of data security would be required?

3.4 Infrastructure

Guiding questions focused on describing the interoperability technology infrastructure and functionalities required by the organization.

- What form of architecture will best fit your organisation's technical interoperability needs?
- Which form of electronic services would your organisation like to provide for exchanging or sharing data?
- Which high-level communication protocol(s) are preferred to exchange data among interoperable systems?
- What form of network is preferred to communicate between interoperable systems?

Section 4 - Interoperability Adoption

Guiding questions directed at establishing the different factors that will influence the adoption of interoperability solutions.

- Are there any collaboration related factors that will influence interoperability adoption?
- Are there any standards related factors that will influence interoperability adoption?
- Which data or information factors will influence the adoption of interoperability?
- Which infrastructure factors will influence the adoption of interoperability?

APPENDIX B – CODE LISTINGS AND INTERVIEW DATA CODING

B.1 Code Listings

Codes of descriptive type were devised to reduce the complexity and increasing the understanding of the raw interview data collected.

The descriptive codes were prepared from the literature reviewed of Coulouris et al. (2009), Somerville (2007) and Tanenbaum et al. (2007) based on the conceptual framework (GIGF) developed. The code listings were revised after examining the data gathered through the interviews. The revised code listings utilised are presented in the tables below.

Table B1: Code List of Distributed Architecture Forms

Codes	Theme
CEA	Collaborative Architecture
CSA	Client-Server Architecture (e.g., Web-based)
DOA	Distributed Object Architecture
PPA	Peer-to-Peer Architecture
NONE	No Distributed Architecture
SOA	Service Oriented Architecture

Table B2: Code List of High-Level Communication Services

Codes	Theme
DRS	Data Replication Services (e.g., Database Replication)
ENS	Event Notification Services (e.g., Triggered Data Transfers)
FTS	File Transfer Services (e.g., FTP, SCP)
MGS	Messaging Services (e.g., JMS, e-Mail)
RPC	Remote Procedure Calls (e.g., RMI and CORBA)
STS	Streaming Services (e.g., Multimedia)
TRS	Transactional Services (e.g., TSQL, PL/SQL)
WS	Web Services (e.g., SOAP and REST)

Table B3: Code List of High-Level Shared Services

Codes	Theme
CNS	Common Naming Services
CWS	Common Workflow Services
DCS	Discovery Services
DIES	Data Import/Export Services
DS	Directory Services
SA	Shared Custom Applications
SMS	Security Management Services

Table B4: Code List of Presentation Formats

Code	Theme
FILE	File (e.g., doc, pdf, xls, txt, csv)
IMG	Image (e.g., jpg, bitmap, png)
JSON	JavaScript Object Notation Text Format
OBJ	Object
XML	Extensible Mark-Up Language Text Format

Table B5: Code List of Security Services

Code	Theme
ATH	Authentication
AUD	Auditing
AUT	Authorization
ENC	Encryption
HASH	Hashing (e.g., MD5)

Table B6: Code List of High-Level Protocols

Code	Theme
FTP	File Transfer Protocol
HTTP	Hypertext Transmission Protocol
NONE	No Protocol
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
VSP	Vendor Specific Protocol

Table B7: Code List of Network Types

Codes	Theme	Ranges	Bandwidths (Mbps)	Examples
LAN	Local Area Network	1-2 Km	10-10000	Ethernet
WAN	Wide Area Network	Worldwide	0.010-600	IP routing
MAN	Metropolitan Area Network	2-50 Km	1-150	ATM
NONE	No Network	-	-	-
WLAN	Wireless Local Area Network	0.15-1.5 Km	2-54	WiFi (IEEE 802.15.1)
WMAN	Wireless Metropolitan Area Network	5-50 Km	1.5-20	WiMax (IEEE 802.16)
WWAN	Wireless Wide Area Network	Worldwide	0.010-2	GSM and 3G

Table B.8: Code List of Organisations

Code	Organisations
MFMR	Ministry of Fisheries and Marine Resources
MHAI	Ministry of Home Affairs and Immigration
MLRR	Ministry of Lands, Resettlement and Rehabilitation
MOF	Ministry of Finance
MOJ	Ministry of Justice
MOLSW	Ministry of Labour and Social Welfare
MOVA	Ministry of Veterans' Affairs
MTI	Ministry of Trade and Industry
MWT	Ministry of Works and Transport
OPM	Office of the Prime Minister

Table B.9: Code List of Information Systems Cases

Code	Information System Names	Owner
ASYCUDA	Automated System for Customs Data and Administration	MOF
BCS	Border Control System	MHAI
CDS	Computerized Deeds System	MLRR
DSA	Daily Subsistence Allowance System	MOF
ECO	Economic Database	MFMR
EDRMS	Electronic Documents and Records Management System	EDRMS
FIMS	Fisheries Information Management System	MFMR
GGFS	Government Garage Fleet Management System	MWT
GPS	Government Payroll System	MOF
GSS	Government Stores System	MWT
HRIMS	Human Resource Information Management System	OPM
IFMS	Integrated Financial Management System	MOF
ICRS	Integrated Company Registration System	MTI
IRS	Inland Revenue System	MOF
LTRS	Land Tax Reconciliation System	MLRR
MSS	Marine Survey System	MFMR
NAMCIS	Namibian Case Management Information Management System	MOJ
NPAS	Namibia Passport System	MHAI
NPRS	National Population Registration System	MHAI
RESDAT	Research Database	MFMR
SWS	Social Welfare System	MOLSW
VETS	Veterans' Information Management System	MOVA

B.2 Interview Data Coding Schemes

Coding of interview data was performed for common themes identified. The different areas and forms of coding used within the IRF are depicted in Tables B.10 and B.11.

Table B.10 Coding Scheme for the Current and Required State of Interoperability

Domains	**Sub-Domains**	**Attributes to Codes**
Collaboration	Organisations/Entities	Table B.8: Organisations
	Information Systems	Table B.9: Information Systems
	Mode	Person/Direct/Indirect
Standards	Interoperability	Yes/No
Data and Information	Shared Data	Yes/No
	Data Presentation Format	Table B.4: Presentation Formats
	Meta-Content	Yes/No
	Common Data Model	Yes/No
	Data Security	Table B.5: Security Services
Infrastructure	N-Tier Interoperability Architecture	Table B.1: Architecture Forms, Table B.3: High-Level Shared Services
	Electronic Services	Table B.2: High-Level Communication Services
	Communication Protocols	Table B.6: High-Level Protocols
	Network	Table B.7: Network Types

Table B.11 Keyword Coding Scheme for Technical Interoperability Adoption Factors

Domains	Adoption Factors	Definition
Collaboration	Agreements	Interoperability agreements between organisations.
	Management Support	Management support for inter and intra organisational interoperability
	Policies	Interoperability policies to guide organisations.
Standards	Appropriate	Standards that are focused at the public service environment.
	Collective Agreement	Public service organisations agree and accept the standards.
	Understandable	Standards formulated should be easy understandable by those who need to conform to them,
Data and Information	Availability	Availability of data to third parties when needed.
	Accountability	Someone should be responsible for the data and be accountable for its correctness.
	Restrictions	Restrictions placed on data by data owners.
	Standards	Data standards relating to structures and content.
	Quality	Quality of data in respect of completeness and correctness.
	Security	Security of data in storage and in transit.
Infrastructure	Availability	Availability of interoperability system by third parties when needed.
	Compatibility	Compatibility of different Information Systems and interoperability solutions.
	Connectivity	Communication infrastructure for connecting data exchange environments.
	Ease of Use	Ease with which interoperability can be established between systems.
	Flexibility	Flexibility with which an interoperable environment can be changed or extended.
	Hosting Platforms	Availability of interoperability middleware hosting platforms for establishing interoperability between systems.
	Performance	Acceptable response and data transfer speed.
	Restrictions	Restrictions placed on establishing interoperability with a system.
	Security	Infrastructure security provided to protect the interoperable environment.
	Skills	Competencies required establishing interoperability and maintaining it.
	Standards	Standards relating to infrastructure development.

APPENDIX C – DATA ANALYSIS CALCULATIONS

The combined summarized results for public service employees interviewed are presented in this section. Interviews were conducted with 26 staff members responsible for 15 Information Systems that formed 12 interoperability Information Systems pairs.

For purposes of clarity and ease of reference, the combined interview results summaries and calculations are presented separately in this appendix for the current state of technical interoperability, required state of technical interoperable and factors that may impact interoperability

The data presented were abstracted from the prepared interview results forms prepared after each interview. The code listings used in coding the data are listed in Appendix B.

C.1 Current State of Interoperability

The combined and summarized interview results data are presented in this section for the 12 pairs of technical interoperable Information Systems identified by interviewees during the interview process. The combined and summarized data for each of the unique pairs of interoperable Information Systems are presented in different tables based on the IRFT (see section 3.5.3) within this section.

The data for this section was obtained from the interview results for the data gathered through section two of the interview guide (see Appendix A).

Table C.1: Summary of Interoperability Information Systems' Pairs

Domains	**Sub-Domains**	**Attributes** (Response and frequency)
Collaboration	Organisations/Entities	MFMR (1), MHAI (1), MOF (5), MOLSW (1), MOVA (1), MWT (1), OPM (1)
	Information Systems	ASYCUDA (1), DSA (1) ECO (1), FIMS (3), GGFS (1), GPS (2), HRIMS (1), IFMS (7), IRS (1), MSS (1), NPRS (1), NPAS (1), RESDAT (1), SWS (1), VETS (1)
	Transfer Mode	PERSON (3), DIRECT (5), INDIRECT (4)
Standards	Interoperability	NO (12)
Data and Information	Shared Data	NO (8), YES (4)
	Data Presentation Format	FILE (8), OBJ (4)
	Meta-Content	NO (12)
	Common Data Model	NO (10), YES (2)
	Security	ATH (4), AUT (4), HASH (8)
Infrastructure	N-Tier Interoperability Architecture	CSA (9), NONE (3)
	Electronic Services	DIES (8), FTS (5), TRS (4), SMS (9)
	Communication Protocols	FTP (5), NONE (3), VSP (4)
	Communication Network	LAN (8), NONE (3), WAN (2)

Table C.1 identifies sub-domain attributes and the number of pairs (5) of Information Systems associated with them.

Table C.2: Interoperable Information Systems Matrix

Information Systems	ASYCUDA	DSA	ECO	FIMS	GGFS	GPS	HRIMS	IFMS	IRS	MSS	NPAS	NPRS	RESDAT	SWS	VETS	Totals
ASYCUDA								X								**1**
DSA								X								**1**
ECO				X												**1**
FIMS			X							X			X			**3**
GGFS								X								**1**
GPS							X	X								**2**
HRIMS						X										**1**
IFMS	X	X			X	X			X					X	X	**7**
IRS								X								**1**
MSS				X												**1**
NPAS												X				**1**
NPRS											X					**1**
RESDAT				X												**1**
SWS								X								**1**
VETS								X								**1**
Totals:	**1**	**1**	**1**	**3**	**1**	**2**	**1**	**7**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**24**

From Table 5.3, each row/column intersections marked with an ‘X’ indicates the different unique pairs of technical interoperable Information Systems.

Table C.3: Summary of Pair 1 (ASYCUDA/ IFMS) Interoperability

Domains	**Sub-Domains**	**Attributes**
Collaboration	Organisations/Entities	MOF
	Information Systems	ASYCUDA and IFMS
	Transfer Mode	INDIRECT
Standards	Interoperability	NO
Data and Information	Shared Data	NO
	Data Presentation Format	FILE
	Meta-Content	NO
	Common Data Model	NO
	Security	HASH
Infrastructure	N-Tier Interoperability Architecture	CSA
	Electronic Services	DIES, FTS, SMS
	Communication Protocols	FTP
	Communication Network	LAN

Table C.4: Summary of Pair 2 (DSA/IFMS) Interoperability

Domains	**Sub-Domains**	**Attributes**
Collaboration	Organisations/Entities	MOF
	Information Systems	DSA and IFMS
	Transfer Mode	INDIRECT
Standards	Interoperability	NO
Data and Information	Shared Data	NO
	Data Presentation Format	FILE
	Meta-Content	NO
	Common Data Model	NO
	Security	HASH
Infrastructure	N-Tier Interoperability Architecture	CSA
	Electronic Services	DIES, FTS, SMS
	Communication Protocols	FTP
	Communication Network	LAN

Table C.5: Summary of Pair 3 (ECO/FIMS) Interoperability

Domains	Sub-Domains	Attributes
Collaboration	Organisations/Entities	MFMR
	Information Systems	ECO and FIMS
	Transfer Mode	DIRECT
Standards	Interoperability	NO
Data and Information	Shared Data	YES
	Data Presentation Format	OBJ
	Meta-Content	NO
	Common Data Model	YES
	Security	ATH, AUTH
Infrastructure	N-Tier Interoperability Architecture	CSA
	Electronic Services	TRS, SMS
	Communication Protocols	VSP
	Communication Network	LAN, WAN

Table C.6: Summary of Pair 4 (GGFS/IFMS) Interoperability

Domains	Sub-Domains	Attributes
Collaboration	Organisations/Entities	MWT and MOF
	Information Systems	GGFS and IFMS
	Transfer Mode	INDIRECT
Standards	Interoperability	NO
Data and Information	Shared Data	NO
	Data Presentation Format	FILE
	Meta-Content	NO
	Common Data Model	NO
	Security	HASH
Infrastructure	N-Tier Interoperability Architecture	CSA
	Electronic Services	DIES, FTS, SMS
	Communication Protocols	FTP
	Communication Network	WAN

Table C.7: Summary of Pair 5 (GPS/IFMS) Interoperability

Domains	Sub-Domains	Attributes
Collaboration	Organisations/Entities	MOF
	Information Systems	GPS and IFMS
	Transfer Mode	INDIRECT
Standards	Interoperability	NO
Data and Information	Shared Data	NO
	Data Presentation Format	FILE
	Meta-Content	NO
	Common Data Model	NO
	Security	HASH
Infrastructure	N-Tier Interoperability Architecture	CSA
	Electronic Services	DIES, FTS, SMS
	Communication Protocols	FTP
	Communication Network	LAN

Table C.8: Summary of Pair 6 (HRIMS/GPS) Interoperability

Domains	Sub-Domains	Attributes
Collaboration	Organisations/Entities	OPM and MOF
	Information Systems	HRIMS and GPS
	Transfer Mode	PERSON
Standards	Interoperability	NO
Data and Information	Shared Data	NO
	Data Presentation Format	FILE
	Meta-Content	NO
	Common Data Model	YES
	Security	HASH
Infrastructure	N-Tier Interoperability Architecture	NONE
	Electronic Services	DIES
	Communication Protocols	NONE
	Communication Network	NONE

Table C.9: Summary of Pair 7 (IRS/IFMS) Interoperability

Domains	Sub-Domains	Attributes
Collaboration	Organisations/Entities	MOF
	Information Systems	IRS and IFMS
	Transfer Mode	INDIRECT
Standards	Interoperability	NO
Data and Information	Shared Data	NO
	Data Presentation Format	FILE
	Meta-Content	NO
	Common Data Model	NO
	Security	HASH
Infrastructure	N-Tier Interoperability Architecture	CSA
	Electronic Services	DIES, FTS, SMS
	Communication Protocols	FTP
	Communication Network	LAN

Table C.10: Summary of Pair 8 (MSS/FIMS) Interoperability

Domains	Sub-Domains	Attributes
Collaboration	Organisations/Entities	MFMR
	Information Systems	MSS and FIMS
	Transfer Mode	DIRECT
Standards	Interoperability	NO
Data and Information	Shared Data	YES
	Data Presentation Format	OBJ
	Meta-Content	NO
	Common Data Model	NO
	Security	ATH, AUT
Infrastructure	N-Tier Interoperability Architecture	CSA
	Electronic Services	TRS, SMS
	Communication Protocols	VSP
	Communication Network	LAN

Table C.11: Summary of Pair 9 (NPAS/NPRS) Interoperability

Domains	Sub-Domains	Attributes
Collaboration	Organisations/Entities	MHAI
	Information Systems	NPAS and NPRS
	Transfer Mode	DIRECT
Standards	Interoperability	NO
Data and Information	Shared Data	YES
	Data Presentation Format	OBJ
	Meta-Content	NO
	Common Data Model	NO
	Security	ATH, AUT
Infrastructure	N-Tier Interoperability Architecture	CSA
	Electronic Services	TRS, SMS
	Communication Protocols	VSP
	Communication Network	LAN

Table C.12: Summary of Pair 10 (RESDAT/FIMS) Interoperability

Domains	Sub-Domains	Attributes
Collaboration	Organisations/Entities	MFMRS
	Information Systems	RESDAT and FIMS
	Transfer Mode	DIRECT
Standards	Interoperability	NO
Data and Information	Shared Data	YES
	Data Presentation Format	OBJ
	Meta-Content	NO
	Common Data Model	NO
	Security	ATH, AUT
Infrastructure	N-Tier Interoperability Architecture	CSA
	Electronic Services	TRS, SMS
	Communication Protocols	VSP
	Communication Network	LAN

Table C.13: Summary of Pair 11 (SWS/IFMS) Interoperability

Domains	Sub-Domains	Attributes
Collaboration	Organisations/Entities	MOLSW and MOF
	Information Systems	SWS and IFMS
	Transfer Mode	PERSON
Standards	Interoperability	NO
Data and Information	Shared Data	NO
	Data Presentation Format	FILE
	Meta-Content	NO
	Common Data Model	NO
	Security	HASH
Infrastructure	N-Tier Interoperability Architecture	NONE
	Electronic Services	DIES
	Communication Protocols	NONE
	Communication Network	NONE

Table C.14: Summary of Pair 12 (VETS/IFMS) Interoperability

Domains	Sub-Domains	Attributes
Collaboration	Organisations/Entities	MOVA and MOF
	Information Systems	VETS and IFMS
	Transfer Mode	PERSON
Standards	Interoperability	NO
Data and Information	Shared Data	NO
	Data Presentation Format	FILE
	Meta-Content	NO
	Common Data Model	NO
	Security	HASH
Infrastructure	N-Tier Interoperability Architecture	NONE
	Electronic Services	DIES
	Communication Protocols	NONE
	Communication Network	NONE

C.2 Required State of Interoperability

This section provides the combined and summarized data extracted from the interview results for the perceived future required state of technical interoperable. This section combines the data gathered through section three of the interview guide (see Appendix A).

Table C.15: Required Collaboration between Organisations Matrix

Organisations	MFMR	MHAI	MLRR	MOF	MOLSW	MOJ	MOVA	MTI	MWT	OPM	Totals
MFMR	X			X							**2**
MHAI		X									**1**
MLRR		X	X	X							**3**
MOF	X	X	X	X	X	X	X	**X**	**X**	**X**	**11**
MOLSW		X		X							**2**
MOJ		X		X		X					**3**
MOVA		X									**1**
MTI		X		X							**2**
MWT				X							**1**
OPM	X	X	X	X	X	X	X	X	X	**X**	**11**
Totals:	**3**	**9**	**3**	**9**	**2**	**3**	**2**	**2**	**2**	**2**	**28**

From Table C.15, row/column intersections indicate the organisations that a specific organisation would like to share data with. Column/row intersections show the organisations that would like to share data with a specific organisation.

Table C.16: Required Interoperable Information Systems Matrix

Information Systems	ASYCUDA	BCS	CDS	DSA	ECO	EDRMS	FIMS	GGFS	GPS	GSS	HRIMS	IFMS	ICRS	IRS	LTRS	MSS	NAMCIS	NPAS	NPRS	RESDAT	SWS	VETS	Totals
ASYCUDA												X											**1**
BCS		X																X	X				**3**
CDS															X				X				**2**
DSA												X											**1**
ECO							X																**1**
EDRMS	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	**21**
FIMS					X											X				X			**3**
GGFS												X											**1**
GPS											X	X											**2**
GSS												X											**1**
HRIMS									X														**1**
IFMS	X			X				X	X	X	X		X	X	X		X		X		X	X	**13**
ICRS																			X				**1**
IRS												X			X								**2**
LTRS												X											**1**
MSS							X																**1**
NAMCIS												X											**1**
NPAS																			X				**1**
NPRS																							**1**
RESDAT							X																**1**
SWS												X							X				**2**
VETS												X							X		X		**3**
Totals:	2	2	1	2	2		4	2	3	2	3	11	2	2	4	2	2	2	8	2	3	2	**64**

From Table C.16, row/column intersections indicate the Information Systems with which an Information System needs to share data. Column/row intersections show the Information Systems that need to share data with a specific Information System.

Table C.17: Summary of Required Information Systems Collaborations

Rank Order	Information Systems	Number of Collaborations
1	EDRMS	21
2	IFMS	13
3	NPRS	8
4	FIMS	4
4	LTRS	4
5	BCS	3
5	GPS	3
5	HRIMS	3
5	VETS	3
6	AYSUDA	2
6	BCS	2
6	CDS	2
6	DSA	2
6	ECO	2
6	GGFS	2
6	GSS	2
6	ICRS	2
6	IRS	2
6	NAMCIS	2
6	NPAS	2
6	RESDAT	2
6	SWS	2
Totals:	**22**	**88**

Table C.18: Summary of Technical Interoperability Requirements Identified

Domains	**Sub-Domains**	**Adoption Factors**	**Total Identified**
Standards	Data and Infrastructure	NO	5
		YES	21
Data and Information	Data Presentation Format	FILE	25
		OBJ	11
		XML	23
	Security	ATH	26
		AUT	20
		ENC	17
		HASH	21
Infrastructure	N-Tier Interoperability Architecture	CSA	19
		PPA	8
		SOA	14
	Electronic Services	DIES	25
		DRS	6
		FTS	25
		RPC	16
		SMS	22
		TRS	11
		WS	22
	Communication Protocols	FTP	25
		HTTP	23
		VSP	15
	Communication Network	LAN	26
		WAN	26

C.3 Interoperability Adoption Factors

The combined and summarized interview results data are presented in this section of the perceived interoperability adoption factors that may influence the establishing of technical interoperability within the public service. This section combines the data gathered through section 4 of the interview guide (see Appendix A) from 26 interviewees.

Table C.19: Summary of Keyword Frequency per Interviewee for the Seven Most Identified Adoption Factors

No.		Keyword Frequencies						
	Data Security	**Data Quality**	**Connectivity**	**Accountability**	**Infrastructure Security**	**Performance**	**Compatibility**
1	1	1	1	1	1	1	1
2	1	1	0	0	0	1	2
3	1	2	2	0	1	2	1
4	2	1	1	0	0	1	2
5	1	0	1	1	0	1	1
6	1	2	2	4	1	0	1
7	1	1	1	1	5	1	0
8	3	1	3	1	1	2	1
9	1	2	1	0	1	1	2
10	2	0	1	1	2	1	1
11	1	1	1	1	1	3	1
12	3	3	2	4	1	1	1
13	1	1	1	1	1	1	1
14	1	1	1	2	2	0	0
15	2	1	1	1	1	0	1
16	1	2	2	1	1	1	1
17	1	1	1	1	1	1	1
18	1	1	1	0	1	0	0
19	1	2	0	3	0	1	1
20	1	1	1	0	1	1	1
21	1	1	1	1	1	0	0
22	1	2	0	1	0	1	1
23	1	0	0	1	0	2	1
24	1	1	1	0	1	1	0
25	1	0	1	0	0	1	1
26	1	1	0	1	2	0	0
Totals:	**33**	**30**	**27**	**27**	**26**	**25**	**23**

Table C.20: Summary of Technical Interoperability Adoption Factors Response Frequencies

Domains	**Adoption Factors** (Keywords)	**Total Identified**	**Responses** (Frequencies)
Collaboration	Agreements	7	10
	Management Support	9	11
	Policies	10	17
Standards	Appropriate	4	11
	Collective Agreement	10	19
	Understandable	8	13
Data and Information	Availability	14	21
	Accountability	18	27
	Restrictions	11	15
	Standards	13	20
	Quality	22	30
	Security	26	33
Infrastructure	Availability	15	17
	Compatibility	20	23
	Connectivity	21	27
	Cost	16	21
	Ease of Use	8	16
	Flexibility	15	19
	Hosting Platforms	13	22
	Performance	20	25
	Restrictions	13	17
	Security	19	26
	Skills	15	17
	Standards	7	14
Total Number of Factors:			**24**

APPENDIX D – INFORMATION SYSTEMS WITHIN THE PUBLIC SERVICE

The summary of Information Systems in use in the Public Service of Namibia was prepared from the data contained within the e-Government Readiness Report (GRN, 2011) and from information obtained from the Office of the Prime Minister, Department of Public Service IT Management.

Table D.1: Summary of Operationalized Information Systems in the Public Service

No.	Public Service Organisation	Number of Information Systems in Use	Number of Information Systems Interoperable
1	Office of the President	1	0
2	Office of the Prime Minister	2	2
3	Office of the Auditor General	3	0
4	Ministry of Justice	6	0
5	National Planning Commission	5	0
6	Ministry of Agriculture, Water and Forestry	5	0
7	Ministry of Defence	2	0
8	Ministry of Education	3	0
9	Ministry of Environment and Tourism	3	
10	Ministry of Finance	4	4
11	Ministry of Fisheries and Marine Resources	4	4
12	Ministry of Health and Social Welfare	11	3
13	Ministry of Home Affairs	5	4
14	Ministry of Labour	1	1
15	Ministry of Lands and Resettlement	5	0
16	Ministry of Mines and Energy	3	0
17	Ministry of Regional, Local Government and Housing	1	0
18	Ministry of Trade and Industry	4	0
19	Ministry of Veterans Affairs	1	0
20	Ministry of Works and Transport	2	2
Totals:		**71**	**20**

APPENDIX E – STRUCTURED WALKTHROUGH RECORD KEEPING

The conceptual CAM, Interoperability Hub and Distribution Architectures were reviewed by OPM e-Government experts through a structured walkthrough process. The purpose of the structured walkthrough was to detect conceptual errors and assess the technical correctness of the architectural designs presented to the review panel.

The organisation and structure of each architectural design were reviewed against the design principles and requirements using different scenarios. Meeting and decision information was recorded and presented using a multipart control sheet template as presented below.

E1. Control Sheet Template

Meeting records were recorded on a standard document template which contained the participants' information, feedback received and decisions taken.

Part A: Initiative Details

Initiative Name:	**Walkthrough Date:**	**Presenter Details:**
Initiative Description:	**Revision Date:**	
	Signed-Off Date:	

Part B: Feedback

Number	Comments and Actions	Date Endorsed
1		
2		

Part C: Decisions

Number	Reviewers	Decisions	Signature
1			
2			

Possible Decisions:

1. Accepted as presented.
2. Accepted with revisions.
3. Revisions that require another walkthrough.
4. Not accepted.