A Proposal of an Information Security Framework for Geospatial Data and Systems Case Study: Abu Dhabi Government

إطار عمل مقترح لأمن المعلومات الخاصة بالبيانات الجيومكانية والأنظمةدراسة حالة من حكومة إمارة أبوظبي

by

HAMDY ELSAYED

A dissertation submitted in fulfilment

of the requirements for the degree of

MSc IT MANAGEMENT

at

The British University in Dubai

Dr. Cornelius Ncube
October 2017

DECLARATION

I warrant that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.

I understand that a copy of my research will be deposited in the University Library for permanent retention.

I hereby agree that the material mentioned above for which I am author and copyright holder may be copied and distributed by The British University in Dubai for the purposes of research, private study or education and that The British University in Dubai may recover from purchasers the costs incurred in such copying and distribution, where appropriate.

I understand that The British University in Dubai may make a digital copy available in the institutional repository.

I understand that I may apply to the University to retain the right to withhold or to restrict access to my thesis for a period which shall not normally exceed four calendar years from the congregation at which the degree is conferred, the length of the period to be specified in the application, together with the precise reasons for making that application.

Signature

oct 24th 2017

Signature of the student

Acknowledgement

First and foremost, I would like to thank God Almighty for giving me the strength, knowledge, ability and opportunity to undertake this challenge and follow through to its completion. It is with the grace of God that this achievement was possible.

Second, I would like to thank my research supervisor “*Dr. Cornelius Ncube”* for his continuous support during my research. *Dr. Cornelius* was always helpful through the different phases of the writing of my dissertation.

Third, I would like to gratefully thank my family for supporting and encouraging me along the entire course of my research. My wife “*Nahla*”, you were standing by my side and spent long nights helping me with the editing and proofreading of this dissertation. My daughter “*Joury*” and son “*Bassem*”, you were the principal source of happiness in my life ever since you entered it, and my motivation during the time of my study and research. My parents “*Kamal* and *Aida*” and sisters “*Abir* and *Ola*”, your prayers were my main source of confidence and success.

Finally, I would like to thank The British University in Dubai for providing with this opportunity, and giving me the chance to study in this world-class environment for research and development. It has been a pleasure meeting such great people from all over the world, from the university staff who provided mentorship and guidance, to my colleagues who became some of my closest friends.

Sincerely,

Hamdy Kamal Elsayed

English Abstract

The purpose of this research is to formulate an information security framework particularly built for the geospatial data and systems in Abu Dhabi governmental entities, taking into consideration the nature and complexity of the geospatial data, techniques required to achieve the security requirements, as well as the influence of users' attitudes and their perceptions about geospatial data security. This research is based on a mixed research methodology; which combines both quantitative and qualitative analysis in order to validate the research's conceptual model, hypothesis, and answer the research questions. Data collection is based on a close-ended-questions survey to users dealing with the geospatial data and an open-ended-questions interview to representatives from AD-SDI governmental entities.

In the conclusion of this research, the proposed security framework is validated and insights are provided on the importance of the behavioural attitude and perceptions of the users in studied organisations towards implementing the geospatial security framework in Abu Dhabi government. Moreover, the research recommends some measures to improve the security of geospatial data in the AD-SDI community and direct them towards secure geospatial data sharing.

نبذة مختصرة

إن الغرض من هذه الدراسة هو إعداد إطار عمل لأمن المعلومات مصمم خصيصاً للبيانات والأنظمة الجيومكانية والتي تستخدم في الجهات الحكومية في إمارة أبو ظبي، مع الأخذ بعين الاعتبار طبيعة وصعوبة تكوين البيانات الجيومكانية، والتقنيات المطلوبة لتحقيق متطلبات أمن المعلومات الجيومكانية، بالإضافة إلى دراسة تأثير سلوكيات المستخدمين وانطباعاتهم عن أمن البيانات والمعلومات الجيومكانية.

ويعتمد منهج البحث لهذه الدراسة على أساليب البحث المختلطة، ويتضمن أساليب التحليل الكمي وأساليب التحليل النوعي ومن ثم يتم التحقق من صحة النموذج النظري الموضوع من قبل الباحث، كما يتم اختبار صحة الفروض الموضوعة والإجابة على الأسئلة البحثية المطروحة. وقد تم جمع البيانات الخاصة بهذا البحث من خلال عمل استبيان لمستخدمي البيانات الجيومكانية باستخدام أسئلة محددة الإجابات، وعقد مقابلات شخصية مع ممثلي مجتمع البيانات المكانية لحكومة إمارة أبو ظبي.

وفي فصل الاستنتاجات، يتم التحقق من صحة إطار العمل المطروح لأمن المعلومات الجيومكانية بالإضافة إلى إثبات أهمية دراسة سلوكيات المستخدمين وانطباعاتهم تجاه تطبيق إطار أمن المعلومات الجيومكانية في مؤسساتهم في إمارة أبو ظبي. كما يتم تعزيز البحث ببعض التوصيات لمستخدمي البيانات الجيومكانية في مجتمع البنية التحتية للبيانات المكانية في إمارة أبو ظبي لتحسين مستوى الأمن للبيانات الجيومكانية وتشجيع المشاركة الآمنة للبيانات الجيومكانية.

TABLE OF CONTENTS

TABLE OF CONTENTS I

LIST OF FIGURES IV

LIST OF TABLES V

ACRONYMS AND ABBREVIATIONS VI

CHAPTER 1. INTRODUCTION 1

1.1 BACKGROUND OF THE STUDY 1

1.2 PURPOSE OF THE STUDY 1

1.3 RESEARCH QUESTIONS 2

1.4 SIGNIFICANCE OF THE STUDY 2

1.5 ORGANISATION OF THE STUDY 3

CHAPTER 2. LITERATURE REVIEW 4

2.1 INTRODUCTION TO CHAPTER 4

2.1 IMPORTANCE OF GEOSPATIAL DATA AND ITS APPLICATIONS 4

2.2 ABU DHABI SPATIAL DATA INFRASTRUCTURE (AD-SDI) AND NEEDS FOR GEOSPATIAL INFORMATION SECURITY 6

2.3 GEOSPATIAL DATA SECURITY FRAMEWORKS 8

2.3.1 Previous Studies Proposed Frameworks for Geospatial Data Security 8

2.3.2 Authentication and Authorization in Spatial Data Infrastructures 10

2.3.3 Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns 11

2.4 OVERVIEW OF INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) AND THE INTERNATIONAL INFORMATION SECURITY STANDARD ISO 27000 12

2.5 OVERVIEW OF ABU DHABI GOVERNMENT INFORMATION SECURITY STANDARDS 13

2.6 INFORMATION SECURITY RISK ASSESSMENT 16

2.6.1 ISO 27001 Risk Assessments 18

2.6.2 Risk Reports 19

2.6.3 Reviews and Monitoring 19

2.7 INSTANCES OF INFORMATION SECURITY IMPLEMENTED POLICIES IN UAE 20

2.7.1 NESA – The New Standard of Information Security in the UAE 20

2.7.2 Dubai Statistics Corporate Information Security Policy Statement 20

2.8 RESEARCH CONCEPTUAL FRAMEWORK AND HYPOTHESES 20

2.8.1 Research Null Hypothesis 20

2.8.2 Conceptual Framework 22

2.9 CHAPTER SUMMARY 22

CHAPTER 3. RESEARCH METHODOLOGY 23

3.1 INTRODUCTION TO CHAPTER 23

3.1 GAPS IN LITERATURE... 23

3.2 RESEARCH DESIGN 24

3.2.1 Research Philosophy 24

3.2.2 Types of Data 24

3.2.3 Research Method.. 24

3.2.4 Research Approach 25

3.2.5 Research Strategy... 25

3.3 SAMPLING PLAN 26

3.3.1 Sampled Population 26

3.3.2 Research Sampling Plan 27

3.3.3 Data Collection Procedure... 27

3.4 ETHICAL CONSIDERATIONS 28

3.5 VALIDITY AND RELIABILITY.. 29

3.6 DATA ANALYSIS PROCEDURE.. 30

3.7 SUMMARY OF THE CHAPTER.. 31

CHAPTER 4. DATA ANALYSIS AND INTERPRETATION 32

4.1 INTRODUCTION TO THE CHAPTER.. 32

4.2 QUANTITATIVE ANALYSIS 32

4.2.1 Descriptive Analysis 32

4.2.2 Inferential Analysis.. 36

4.2.3 Hypothesis Results.. 42

4.3 GAP IN QUANTITATIVE ANALYSIS 44

4.4 QUALITATIVE ANALYSIS 44

4.4.1 Respondents' Profile 44

4.4.2 Role of AD-SDI Community in Geospatial Data Sharing of Organisations........... 45

4.4.3 Challenges Related to Data Security.. 47

4.4.4 Strategies to Mitigate Geospatial Data Security Risks........................... 48

4.5 SUMMARY OF THE CHAPTER 51

CHAPTER 5. CONCLUSION 52

5.1 INTRODUCTION TO CHAPTER 52

5.2 DISCUSSION OF RESEARCH QUESTIONS 52

5.3 RECOMMENDATIONS TO GOVERNMENTAL ENTITIES IN THE CONTEXT OF GEOSPATIAL DATA SECURITY 57

5.4 SUMMARY AND RECOMMENDATIONS FOR FUTURE SCOPE 58

REFERENCES 59

APPENDIX 1: QUANTITATIVE QUESTIONNAIRE 63

APPENDIX 2: QUALITATIVE QUESTIONNAIRE 71

APPENDIX 3: ORGANISATION'S STRATEGIC POSITION CORRELATION 74

APPENDIX 4: ORGANISATION'S STRATEGIC POSITION COEFFICIENTS 78

APPENDIX 5: ORGANISATION’S PERCEIVED CONTROL CORRELATION 82

APPENDIX 6: ORGANISATION’S PERCEIVED CONTROL COEFFICIENTS 86

LIST OF FIGURES

Figure 2-1: Different aspects of AD-SDI 7

Figure 2-2: Zope-Chaudhari & Venkatachalam`s Framework 9

Figure 2-3: Bertino`s Framework for Geospatial Data Security 10

Figure 2-4: Background, terms and definition of ISO 27000 standard family 13

Figure 2-5: Abu Dhabi Information Security Framework 15

Figure 2-6: Elements of Risk Assessment 16

Figure 2-7: The Proposed Conceptual Framework 22

Figure 4-1: Age and gender frequency distribution 33

Figure 4-2: Frequency distribution of user's education qualification 33

Figure 4-3: Frequency distribution of the users at each level involved in study .. 34

Figure 4-4: Frequency distribution of the experience of the respondents 34

Figure 5-1: Conceptual Framework of Geospatial Information Security 53

Figure 5-2: A Breakdown of The Organisational Requirements of The Suggested Geospatial Information Security Conceptual Framework 54

Figure 5-3: A Breakdown of The Technical Requirements of The Suggested Geospatial Information Security Conceptual Framework 54

LIST OF TABLES

Table 4-1: Users behavioural attitudes on geospatial data sharing 35

Table 4-2: Correlation between strategic position and sharing behaviour 37

Table 4-3: Linear regression model summary 38

Table 4-4: Analysis of variation table to check the significance of the model 38

Table 4-5: Model summary of regression model 40

Table 4-6: Analysis of variation table to check the significance of the model 41

Table 4-7: General information of the participants involved in the study 45

ACRONYMS AND ABBREVIATIONS

AD	Abu Dhabi
SDI	Spatial Data Infrastructure
ISMS	Information Security Management System
ISO	International Standards Organisation
ADSIC	Abu Dhabi Systems and Information Centre
UN-GGIM	United Nations- Global Geospatial Information Management
AGEDI	Abu Dhabi Global Environmental Data Initiative
DMA	Department of Municipal Affairs
ADWEA	Abu Dhabi Water and Electricity Authority
MSD	Military Survey Department
DPE	Department of Planning & Economy
ADNOC	Abu Dhabi National Oil Company
EAD	Environment Agency - Abu Dhabi
FGDS	Fundamental Geographic Data Sets
GIS	Geographic Information System
RBAC	Role-based Access Control
OBS	Object-Based Storage
ISRAM	Information Security Risk Analysis Method
DEMATEL	Decision Making Trial and Evaluation Laboratory
ANP	Analytic Network Process
NESA	National Electronic Security Authority
NGO	Non-Government Organisation
SOP	Standard Operating Procedure
KPI	Key Performance Indices
MS	Microsoft
SPSS	Statistical Package for Social Science
ANOVA	Analysis of variance
H_0	Null hypothesis
PDCA	Plan-Do- Check-Act
ISO/IEC	International Standards Organisation/ International Electrotechnical Commission
CISO	Chief Information Security Officer

CHAPTER 1. INTRODUCTION

1.1 Background of The Study

Abu Dhabi Government is currently running many initiatives that aim for the transformation towards smart government, so all government services could be provided through internet portals and smartphones applications. With the computer networks revolution and the spread of online services everywhere in the world, the risk of having sensitive information stolen by unauthorized internal or external users had to be considered. Hence, the government established the topic of information security as one of the governmental business management priorities.

As Abu Dhabi governments become smarter and data sharing initiatives are undertaken, the importance of having smart systems and platforms connected and available twenty-four hours to the public emerges. Those systems must also deliver high quality and instantly responsive services that keep the information shared; transmitted and received, secured adequately.

1.2 Purpose of The Study

Each government entity in Abu Dhabi government maintains its own data and systems; such data types could be business transactions, employees' information, organisational assets, etc. Geospatial data is considered one of the most important data stored on the government information systems. Geospatial data is data that includes geographic information to determine the exact location of certain features on the ground. Those features might be trees, traffic signs, private properties, underground cables, fire extinguisher, etc.

Each entity in the government is responsible for keeping the business data and assets on its information systems accessible and secure. For instance, the Department of Transport keeps information about traffic and street signs in their database, while the Department of Municipal Affairs maintains all land plots and their ownership information in its geographic database. The confidentiality and security classification of the data is the responsibility of each data owner. For example: street signs dataset is classified as public data and any access to this dataset will not affect the organisation business since it is already known and available to the public. On the other side, private property ownership is considered highly confidential information that must be secured and only accessible to authorized users.

The purpose of this study is to propose a security framework that helps the governmental entities in keeping geospatial data secure and only accessible to authorized users. Achieving this purpose will help the government of Abu Dhabi to encourage its entities to participate in data sharing initiatives among the governmental entities without fearing the risk of getting into any security issues.

1.3 Research Questions

The research questions of this study have been constructed based on the initial study of the current situation in Abu Dhabi government, in the context of geospatial data security as follows:

- Can security applications and technology be sufficient to overcome security challenges in the context of geospatial information? What other areas can we look into?
- What is the role of users' behavioural attitude, strategic positions and perceptions, and internal and external control factors on geospatial data sharing in the context of security?
- How can the process followed to assess and treat the risks associated with geospatial data in AD-SDI help encourage users and entities to embrace geospatial data sharing?
- How can data classification as well as related users' access rights affect perceived security issues in the context of geospatial data sharing?

1.4 Significance of the study

Abu Dhabi government has published "Abu Dhabi Government Security Standard", followed by a program that was launched to start implementing the standard in all of Abu Dhabi's governmental entities to ensure the security of the data sets and systems being used on daily basis in the government. Due to the fact that the geospatial data is different and more complex in structure than any other data format, the implementation of the standard was a bit challenging and has reflected negatively and caused some resistance among governmental entities where data sharing is concerned.

This research will introduce a framework, insights, and recommendations to ensure geospatial data security whether the data is static (stored on servers) or dynamic (shared or exchanged with other entities). Accordingly, this research will help the government overcome common entities’ resistance towards sharing data because of fears of the consequences of inadequate data security.

1.5 Organisation of The Study

This study is divided into five main chapters, followed by seven appendices. Chapter one is an introduction to the research, its background, and high-level information about the research. Chapter two includes the literature review about information security and local related information. Chapter three presents the methodology used in this research and the used validation and verification techniques during data collection, analysis, and conclusion. Chapter four furnishes the data collection and analysis part, which consists of two main sections, namely; quantitative and qualitative analysis. Finally, chapter five draws the conclusion from the study and suggests future opportunities in the research topic.

The seven appendices attached to the study include the qualitative and quantitative questionnaires used in data collection, as well as the statistical tables that have been exported from the software used in data analysis.

CHAPTER 2. LITERATURE REVIEW

2.1 Introduction to Chapter

Spatial techniques and concepts are often considered crucial for retrieval and indexing of images and videos from multimedia databases. Geospatial data is also referred to as geo-data or GIS (Geographic Information System) data that includes explicit geographic positioning data contained in the information, such as network of roads, mining information, images from geo-referenced satellite, aeroplane, or ground vehicle. This chapter provides an overview on the geospatial data and its applications as well as an overview on Abu Dhabi Spatial Data Infrastructure (AD-SDI) and requirements for geospatial information security to ensure the confidentiality, integrity, and availability of the data shared among the AD-SDI entities. This section of the dissertation also presents a conceptual framework for geospatial data security that includes authentication, authorization, and security guidelines for geospatial data and information systems. In addition, it includes a brief discussion on establishing Information Security Management Systems (ISMS) and ISO 27000 security standard.

2.1 Importance of Geospatial Data and Its Applications

Geospatial data is data that has geographic attributes, i.e., this type of information has multiple record fields, such as; longitude-latitude coordinates, address, city, and postal code included in them. In other words, it can be said that the geospatial data includes attributes that describe geographical features in the dataset. This data has many forms and has more complex structure than tabular or geometric data (Geospatial World, 2010). It is considered a subset of spatial data, that indicates locations within a specific coordinate system.

There are two basic types or forms of geospatial data– first, vector data; which uses lines, points, and polygons for representing the ground features like cities, roads, etc., and provides more accurate results than the other forms (Mathworks.com, 2017). Second, raster data; which uses cells (dots or pixels used by computers) for representing the spatial features’ attributes. The cities’ names are represented by single cells, roads are represented by linear sequential cells, and clusters of adjacent cells represent streams. This type of geospatial data is often used in the georeferenced remote sensing satellite or aerial photos. It provides faster results than vector form (Mathworks.com, 2017).

Geospatial data is different from the other kind of spatial data as it is absolutely/relatively geo-referenced, in other words, positioned on a plane, there lies the importance of this kind of spatial data. It has a terrestrial coordinate system that transforms to multiple local coordinate systems. The geospatial data collection and information infrastructure can be included into the official reporting systems to ensure adequate human capacity building and maintaining topographical inventory (Shekhar et al., 2002). There are many applications of geospatial data and some of them include:

Reviewing Facilities and Assets: The geospatial data can help in maintaining the administrative core division for national topography and transportation. It could be used in making systematic inventory and critically mapping the national infrastructure and facilities such as, hospitals, health clinics, schools, water resources, irrigation systems, public transportation, tourist spots, agricultural facilities and waste treatment facilities (Mishra & Coulibaly, 2009).

Access to Satellite Imagery: Shekhar et al. (2002) observed that the report presented by most of the countries across the world have access to only low-resolution satellite imagery as the higher resolution satellite imagery is quite cost prohibitive. The use of geospatial data can provide affordable access and wide scale utilization of moderate to high resolution satellite imagery for nations on a regular basis.

Remote Sensing: The pairing of remote sensing with geospatial data can be crucial in addressing environmental disasters and public health concerns. As per Shekhar et al. (2002), geospatial data applications in remote sensing can be used in the ecological situation monitoring such as air and water quality monitoring, rising sea levels, shrinking river banks, etc.

2.2 Abu Dhabi Spatial Data Infrastructure (AD-SDI) and Needs for Geospatial Information Security

The Government of Abu Dhabi has administered a program known as Abu Dhabi Spatial Data Infrastructure (AD-SDI) within the e-government programme of Abu Dhabi Systems and Information Centre (ADSIC) for facilitating geospatial data sharing amongst governmental agencies and various stakeholders. Before 2008, governmental entities in Abu Dhabi working in different sectors used to collect geographic information of different locations separately. Collection of approximately similar information usually consumed a lot of time, cost, and data storage. Also, the collected data had a lot of duplication, less clarity, and many other issues which led to the formation of AD-SDI program.

One of the long-term targets of AD-SDI is providing a seamlessly interoperable network that will allow various agencies to share data with one another. This will enable the use of geospatial data in various e-Government services through linking, sharing and coordinating. AD-SDI is the latest strategy of the government, developed using best international practices and standards. It is developed to be cutting edge geo-information system and technology that is being used to produce the base mapping data for the entire Abu Dhabi Emirate and more refined mapping for the most developed areas (UN-GGIM, 2016)

It has also aided in increasing the use of Abu Dhabi Global Environmental Data Initiative (AGEDI) for quality environmental data collection. The Department of Municipal Affairs (DMA) and Abu Dhabi Water and Electricity Authority (ADWEA) have used this technique for updating their mapping programs and developing distribution facilities' information respectively. Some of the partner agencies of AD-SDI are Military Survey Department (MSD), The Department of Planning and Economy (DPE), Etisalat (Telecommunications Company), Abu Dhabi National Oil Company (ADNOC), Environmental Agency Abu Dhabi (EAD) and more (UN-GGIM, 2016). These agencies develop framework data i.e., Fundamental Geographic Data Sets (FGDS), which form the basis of GIS activities. The data collected from these agencies forms the nucleus of AD-SDI's cell of data-sharing. AD-SDI covers three main components of SDI that are data, technology, and services, and is spanned over different aspects that are depicted in Figure 2-1.

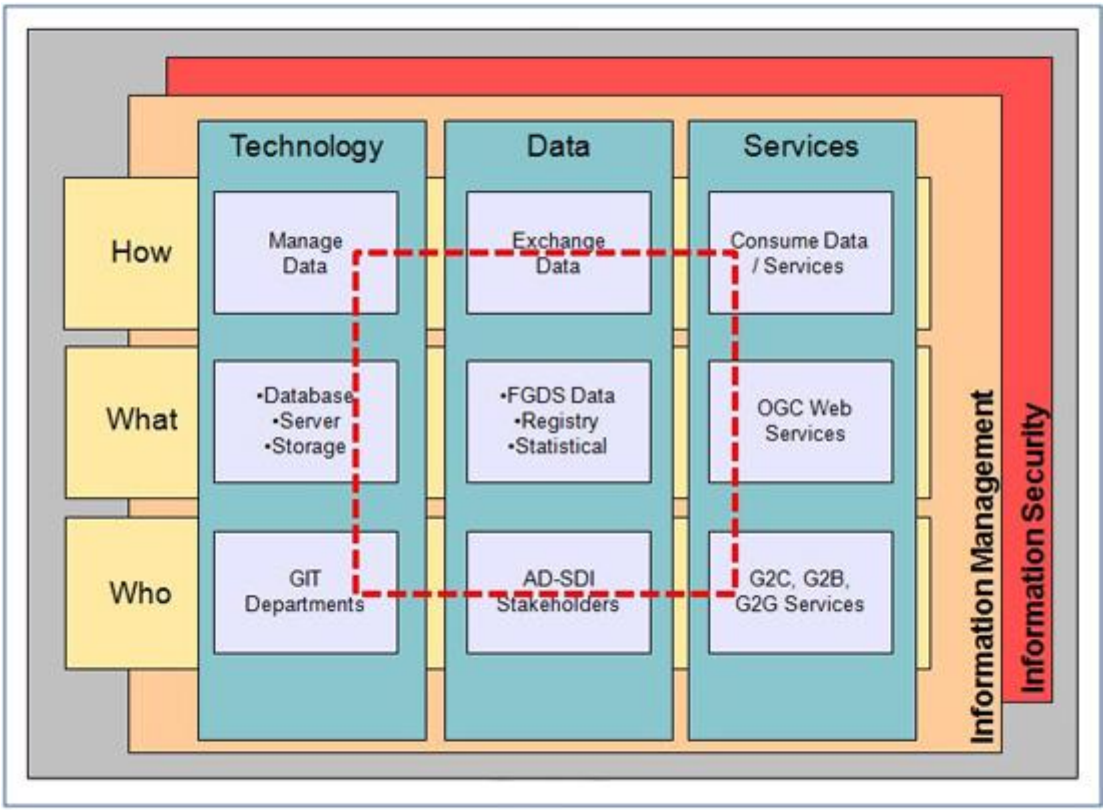


Figure 2-1: Different aspects of AD-SDI

Source: (AD-SDI n.d.)

According to Wang & Wang (2006), geospatial information security basically depends upon the built-in mechanism for security or protection mechanism of the components such as; database, operating system, etc. The authors noted that the major challenge here is the complexity associated with the geospatial information in GIS that makes it difficult to manage the integrated security-protecting mechanism, as well as increases the workload and decreases security. Some of the security and privacy concerns associated with geospatial information are the issue of data confidentially and secrecy, non-provisional key distribution, extremely time sensitive data, etc.

In the opinion of Boxall (2005), the popularity of geospatial information has risen tremendously and steadily. Consequently, the availability of geospatial data has substantially increased, and security changes have been essential to protect the interests of those who seek this information. The protection of geospatial information from a wide range of threats is essential for protecting national security, national defence institutes, and environmental interests. Kussul et al. (2010) have assessed the security risks associated with the heterogeneous geospatial information and developed a risk assessment system that consists of an integrated intelligent system for monitoring and controlling the flow of information in crisis.

2.3 Geospatial Data Security Frameworks

With the development of Geographic Information Systems, the security of geospatial data has become more and more vital because of the increase in geospatial data sharing and inter-operability. (Ma et al., 2010) have addressed the issue of access restrictions of geospatial data and discovered that existing technologies are inadequate in fulfilling the security requirements of spatial data. The authors have presented an authorization mechanism for access control based on Role-Based Access Control (RBAC) model. Wang & Wang (2006) have proposed the use of Role-Based Access Control (RBAC) in the framework of GIS software through the introduction of the "role" concept; managing users' privileges systematically, and combining PKI/PMI systems for safety issues related to spatial information.

2.3.1 Previous Studies Proposed Frameworks for Geospatial Data Security

According to Zope-Chaudhari & Venkatachalam (2013), geospatial data is a vital part of a smart government, however, confidentiality, security, and privacy are major concerns. Therefore, it is necessary to consider the characteristics of geospatial data whilst developing security policies. The authors proposed a geospatial data security framework as depicted in Figure 2-2. This framework has two security layers, namely; the internal layer and the outer layer. The internal layer is the storage layer that deals with the details and flexibility of access control in geospatial database, and only allows authentic data outsourcing for transforming geospatial data to trustworthy servers that also facilitates privacy management. The second layer is the outer layer, also known as distribution layer, that deals with users' interaction amongst themselves and their interaction with trusted servers or

GIS web services for retrieving geospatial data that safeguards the system against any unauthorized access or malicious attacks.

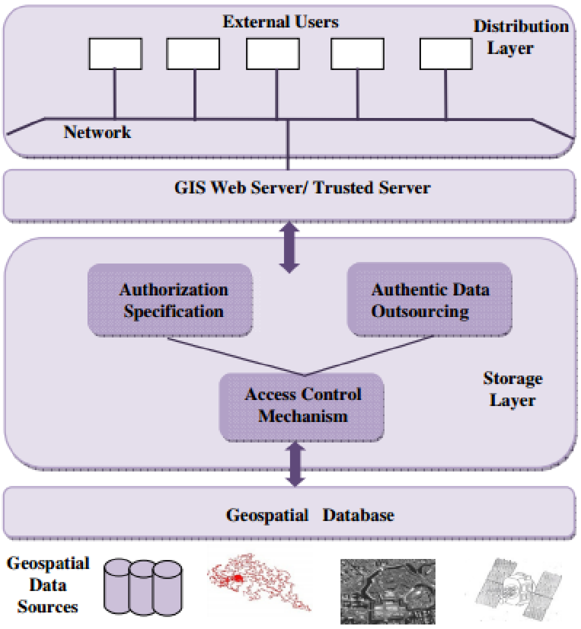


Figure 2-2: Zope-Chaudhari & Venkatachalam`s Framework

Source: (Zope-Chaudhari & Venkatachalam, 2013)

Bertino et al. (2008) described some of the most relevant elements associated with geospatial data security, namely; security policy specification and reasoning framework (including the ability to express different kinds of spatio-temporal and geospatial data, support for diverse modification rights and diverse data access, determination of redundant and inconsistent policies, etc); interoperability of security policies (in order to ensure a feasible privacy and security approach for real-world applications and developing specialized mapping services) and trust, privacy, and integrity. The conceptual framework presented by the authors is depicted in Figure 2-3.

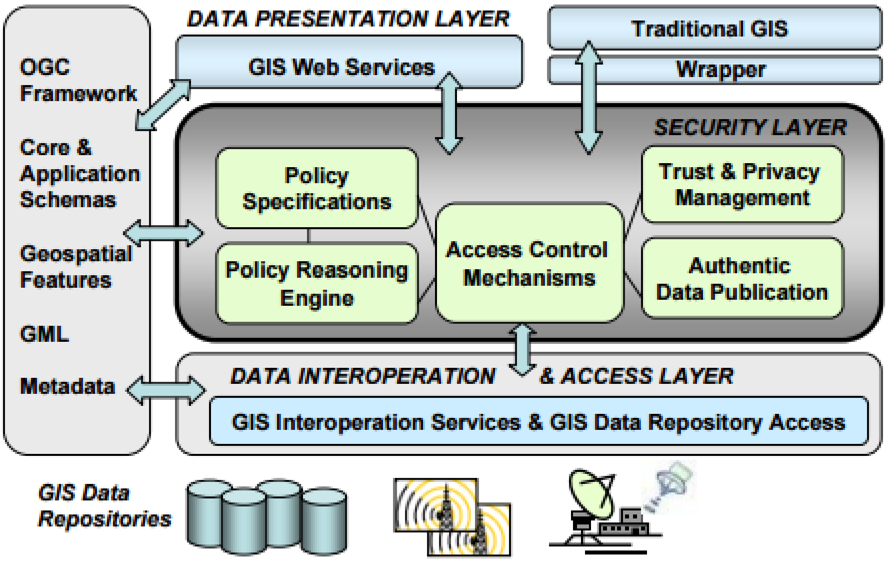

OGC Framework
Core & Application Schemas
Geospatial Features
GML
Metadata
DATA PRESENTATION LAYER
GIS Web Services
Traditional GIS
Wrapper
SECURITY LAYER
Policy Specifications
Policy Reasoning Engine
Access Control Mechanisms
Trust & Privacy Management
Authentic Data Publication
DATA INTEROPERATION & ACCESS LAYER
GIS Interoperation Services & GIS Data Repository Access
GIS Data Repositories

Figure 2-3: Bertino`s Framework for Geospatial Data Security

Source: (Bertino et al., 2008)

Zhang & Wang (2008) proposed a security management model for geospatial data in the context of the Geographical Information Systems' unsolved problem. The new storage model proposed for distributed GIS was spatial data based and an Object-Based Storage (OBS) has been constructed for it that provided an integrated solution for both secure data sharing and high-performance storage services. The model proposed consisted of three security protocols namely, GIS Server-Security Manager protocol, GIS Server-OBSD protocol, and Security Manager-OBSD protocol, for maintaining privacy, integrity, and confidentiality of GIS spatial data.

2.3.2 Authentication and Authorization in Spatial Data Infrastructures

Amongst the most relevant aspects of information security systems are authentication and authorization. Authentication can be defined as assurance provision that claims an entity's identity; it describes the verification of the communication partner. The concept of authentication is described as passive while validating the credibility and active while entity authenticates itself. Authorization is another key security requirement that controls the access to the resources; the data access requests are matched with policies to define access right to the resources (Schäffer, n.d.).

2.3.3 Secure Geospatial Data Access Guidelines

Geospatial data is originated and disseminated amongst many private, public and non-profit organisations. Dissemination of data is crucial for many organisations and the majority of geospatial data is appropriate for public access. On the other hand, there is a small section of geospatial data that could pose security and privacy risks and thus, requires special safety measures (FGDC, 2005). Sensitive geospatial information is generally safeguarded using different decision criteria and procedures, some of the standard guidelines are:

First, sensitive geospatial information content is identified to determine the associated security threats that might happen. Second, setting the relevant mitigation plan, which is regularly reviewed in a process called risk reassessment, so a decision might be made -if needed- to enforce the proper safety measures for protecting geospatial data.

In addition to this, these guidelines also provide a way for balancing off security risks whilst maintaining the advantages of geospatial data distribution. These guidelines also aid in selecting apt risk-safety measures for organisations, so that they can access geospatial information whilst maintaining the integrity and secrecy of sensitive information. These guidelines apply to geospatial information irrespective of their access method, format and delivery method (FGDC, 2005). According to the security guidelines, security decisions are based on the following three factors: risk to security, where the usefulness of the data could be a reason for choosing it as a particular potential target or for executing or planning any attack on potential target (FGDC, 2005). The second is the uniqueness of information, where the information contained could pose a threat to security or is sensitive information that should be not available for all (FGDC, 2005). The third is the total advantage of distributing data, where the measure of social benefits of distribution information is weighed versus the security risk posed by them (FGDC, 2005).

The guidelines also suggest two safety measures such as, removing or modifying sensitive information and reviewing the changed data for effectively dealing with security risks (FGDC, 2005). Further, restricting the data through commiserating the assessed risk and establishing restrictions on access, use, or redistribution of data (FGDC, 2005).

2.4 Overview of Information Security Management System (ISMS) and The International Information Security Standard ISO 27000

Information Security Management System (ISMS) can be defined as a set of procedures and policies for the systematic management of sensitive data or information in any organisation. The main objective of ISMS is minimizing the associated risks and ensuring smooth business practices by advanced prevention and limiting of security breach impact. These security management systems mainly address the behavioural issues of the employees, data processing techniques and technological components used. The ISMS also assesses the risks associated with establishing, implementing, operating, monitoring, reviewing, and maintaining the information security of the organisation.

The ISMS can mainly be targeted towards securing any kind of datasets, such as payment data, consumer data, etc. Or they can be comprehensively implemented to be integrated in the working culture of the company. Some of the major benefits of ISMS that it targets the data security for both the organisation and its consumers. It also ensures business risk handling by security control implementation to enhance productivity of both the employees and the organisation along with an improved corporate image (IRQS, 2013).

ISO 27000 security standards are the specifications used for creating an Information Security Management System. This standard does not provide instructions for specific actions, but rather includes suggestions on the documentation of data, conduction of internal audits, continual improvement programs, and preventive and corrective measures. The certification provided by this standard mainly includes the intended scrutiny of the information assets of the organisation, and a risk estimation process related to the assets is performed.

The process measures the probability of entire system failure or external attack, and the impact such events would have on the organisational structure. It also evaluates the effectiveness of the system placed to protect such assets and the overall security and reliability of the entire system. The main benefit of this standard lies in increasing the credibility of businesses amongst consumers and business partners (Disterer, 2013).

Along with that, it is independent demonstration of regulations and laws, conformity with legislation, better management control, and competitive advantage that are the main benefits of the standard’s benefits. Additionally, it aids in contingency planning, improved risk management, reduction in security risks and breaches, cost effectiveness, and consistent security (Zarki et al., n.d.). Figure 2-4 depicts the background, terms and the definition of ISO 27000 standard family.

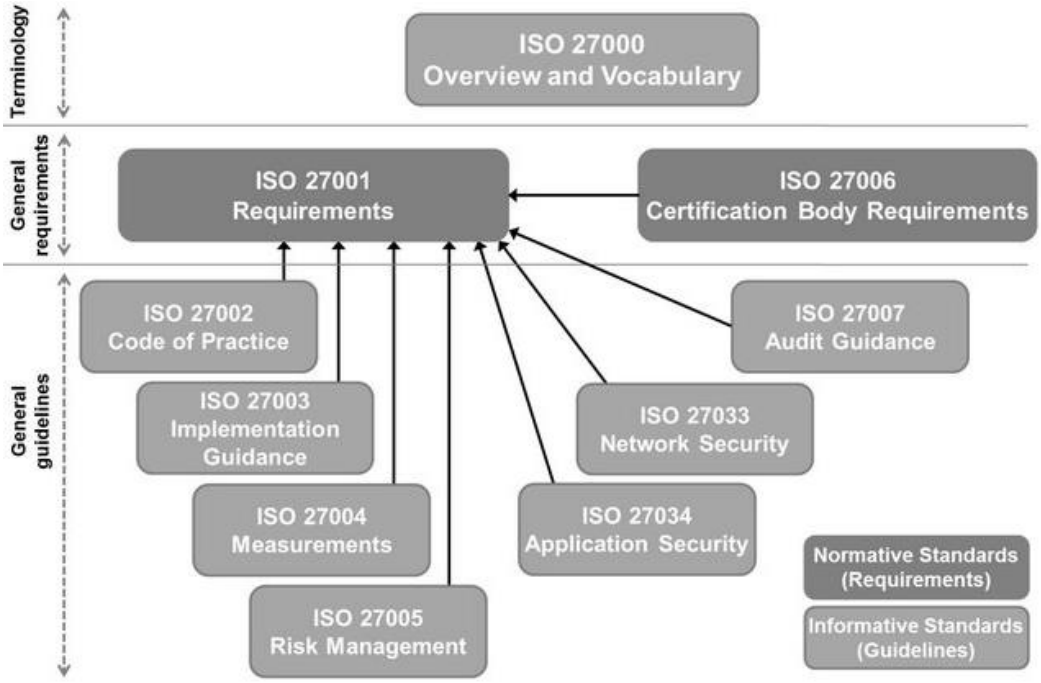

Terminology
General requirements
General guidelines
ISO 27000 Overview and Vocabulary
ISO 27001 Requirements
ISO 27006 Certification Body Requirements
ISO 27002 Code of Practice
ISO 27003 Implementation Guidance
ISO 27004 Measurements
ISO 27005 Risk Management
ISO 27007 Audit Guidance
ISO 27033 Network Security
ISO 27034 Application Security
Normative Standards (Requirements)
Informative Standards (Guidelines)

Figure 2-4: Background, terms and definition of ISO 27000 standard family

Source: (Disterer, 2013)

2.5 Overview of Abu Dhabi Government Information Security Standards

In year 2005, Abu Dhabi Systems and Information Centre (ADSIC) was launched by the government of Abu Dhabi, and one of the most important objectives of its establishment is the implementation of information control and security in governmental agencies of Abu Dhabi. With implementing the information security controls and fulfilling the standard’s requirements, organisations can follow government regulations, protect information assets, comply with Abu Dhabi government security regulations, increase awareness about information security, provide secure and effective services, and enhance credibility amongst external users and partners (Systems and Information Centre, 2017). The other key mandates of ADSIC (UN-GGIM, 2016) are as follows:

- Supporting data sharing, limiting data redundancy and cutting costs by geographic data development and alignment
- Ensuring that government laws, legislations, practices and policies support maximum information exchange and coordination.
- Providing better alternatives for evaluation in decision-making processes and enhancing coordination.

The Information Security Standards of Abu Dhabi supports governmental agencies in embedding and implementing an Information Security framework as depicted in Figure 2-5 showcasing the key elements of the framework. The benefits of this framework lie in gaining an integral perspective on the information security system’s capabilities that is to be deployed or maintained (ADSIC, 2013). In Figure 2-5 below, individual entities are expanded in more detail for relevant areas of Control Standards section.

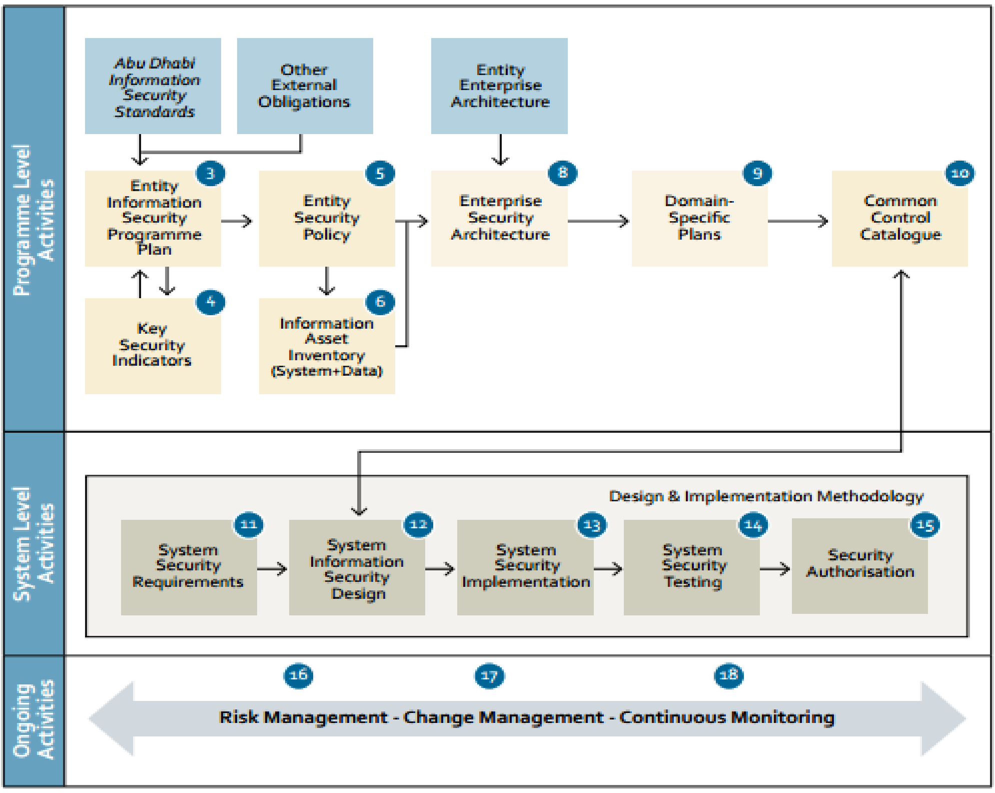

Programme Level Activities
Abu Dhabi Information Security Standards
Other External Obligations
Entity Enterprise Architecture
3 Entity Information Security Programme Plan
5 Entity Security Policy
8 Enterprise Security Architecture
9 Domain-Specific Plans
10 Common Control Catalogue
4 Key Security Indicators
6 Information Asset Inventory (System+Data)
System Level Activities
Design & Implementation Methodology
11 System Security Requirements
12 System Information Security Design
13 System Security Implementation
14 System Security Testing
15 Security Authorisation
Ongoing Activities
16
17
18
Risk Management - Change Management - Continuous Monitoring

Figure 2-5: Abu Dhabi Information Security Framework

Source: (ADSIC, 2013)

There are three main activities described in this framework, namely; ongoing activities, system level activities, and program level activities. The program level activities include: Abu Dhabi Information Security Standards, Entity Information Security Program Plan, Key Security Indicators, Entity Information Security Policy, Information Asset Inventory, Enterprise Information Security Architecture, Domain Specific Implementation Plans, Common Control Catalogue, and other external obligations. The system level entities are Security Requirements of Information Systems, Information Security Design, testing, authentication and implementation. The ongoing activities are: risk, change management, and continuous monitoring (ADSIC, 2013).

2.6 Information Security Risk Assessment

One of the crucial elements of information security management are risk management activities. Risk management activities involves establishing a focal point of central management, implementing suitable policies and controls, spreading awareness, and evaluating and monitoring the effectiveness of policies and controls. It is important to note that all the elements associated with risk management are crucial, as risk assessments is the fundamental to the entire security management. Particularly, it is the basis for implementing appropriate policies and choosing cost-effective methods to implement such policies (GAO, 1999). The threats and risks are changeable with time; hence it is vital to conduct risk reassessment on a periodic basis to reconsider the effectiveness and suitability of the selected policies and controls. The continuous cycle is of risk assessment is depicted in the following Figure 2-6:

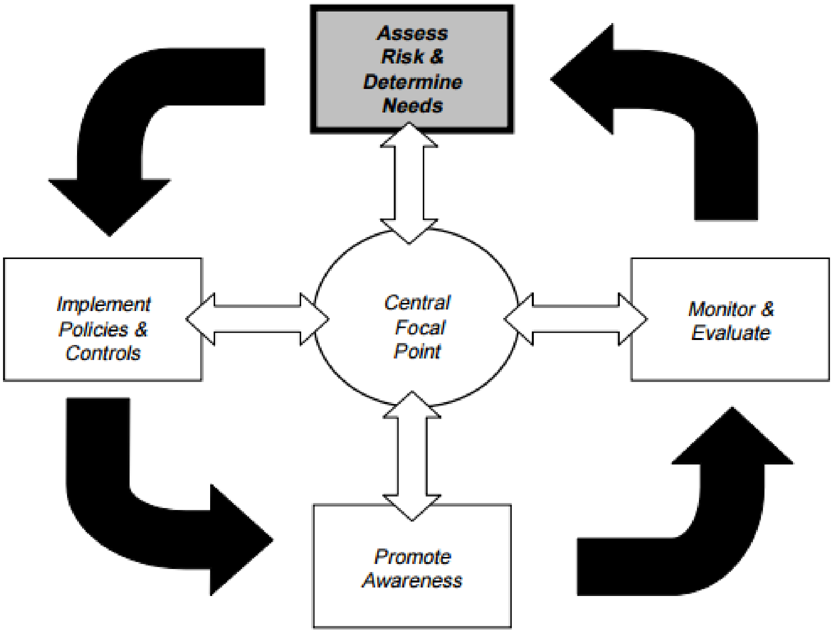


Figure 2-6: Elements of Risk Assessment

Source: (GAO, 1999)

Zhang & Wang (2008) presented a paper on information security engineering and described risk assessment as a crucial part of it. This paper discusses the elements of risk assessments such as: current situation, security models, security standards, and processes and methods, after that information security evaluation is conducted. Bernard (2007) studied on Information Lifecycle Security Risk Assessment, which is a tool for finding security gaps. Most of the programs for information security includes physically protecting the infrastructure of the information system but it does not physically protect the information. Thus, this makes the information vulnerable to risks and threats. This paper presents an information security program that encircles all stages of critical data form its generation to storage to destruction. This method integrates both physical and electronic information elements to mitigate security risks.

Karabacak & Sogukpinar's (2005) study was based on an information security risk analysis method known as ISRAM, to address the continuously changing technological environment for information security risk assessment. The authors had used multiple quantitative and qualitative risk assessment methods to analyse the information security risks along with ISRAM. The results have indicated that ISRAM provides more consistent results over a particular period of time, as it includes participation of staff and managers of the organisation. Lo & Chen (2012) studied a hybrid information security risk assessment method for determining interdependences between controls. This hybrid procedure evaluates risk levels associated with information security through various proposed security controls. As a first step, this method applies the approach called Decision Making Trial and Evaluation Laboratory (DEMATEL) for constructing interrelations between control areas. The second step involves the calculation of the probability Analytic Network Process (ANP) method for collecting feedback and detecting interdependences between security control functions in real life situations. The last step uses the Fuzzy Linguistic Quantifiers-guided Maximum Entropy Order-Weighted Averaging (FLQ-MEOWA) operator for expert calculation of aggregate impact values to reduce influence of extreme evaluations. This hybrid method was tested with real life application in branch office of health insurance institute, Taiwan and the results confirmed that this method can detect major factors amongst security control.

2.6.1 ISO 27001 Risk Assessments

ISO 27001is the international standard which specifies the details of an information security management system (ISMS), providing best practices covering people, processes and technology in the information security context. Information security risk assessment and management are part and parcel of ISO 27001.

Risk Assessment in the context of ISO 27001 is done through a five-step process (ITGovernance, 2017).

2.6.1.1 Establish a Risk Management Framework

These are the directions followed to identify risks, assign risk ownership, study risks' implications on security, validity, and accessibility of data, and calculate estimated impact and likelihood of risks. Most importantly, risk assessment should start with the study of four aspects in the organisation: Baseline security criteria, Risk scale, Risk appetite, and Scenario or asset-based risk assessment.

2.6.1.2 Identify Risks

Identifying risks that might impact the confidentiality, integrity and availability of information is the longest step in the risk assessment process. It is advised to use asset-based risk assessment by creating a list of information assets and study the risks associated with them.

2.6.1.3 Analyse Risks

Risk analysis is performed by examining all the possible threats and liabilities associated with each asset. For example, in the case of the loss of a cell phone, the liability needs to be studied in terms of impact and likelihood and assign a value to each of those aspects based on your risk criteria.

2.6.1.4 Evaluate Risks

Risks are then evaluated by being weighed against acceptable risk levels, based on the information collected in the risk management framework created in the first step. Then risks are ordered according to their priority and which risk should be handled before the other.

2.6.1.5 Select Risk Treatment Strategy

According to the nature of each risk, a suitable strategy is selected to treat it. The risk can either be: Avoided; by completely erasing it, Mitigated; by using one of the organisation's security standards, Shared or Transferred to other parties like insurance, or Accepted in case it can be allowed by the framework created in step 1.

2.6.2 Risk Reports

ISO 27001 for information security risk assessment dictates the creation of a number of reports, as a part of the auditing and certification process, the most important of which are the Statement of Applicability (SoA) and the Risk Treatment Plan (RTP).

2.6.3 Reviews and Monitoring

Another requirement dictated by the ISO 27001 is the ongoing review, update and improvement of the ISMS to ensure continued functionality and versatility. Additionally, audits are held and require the ISMS to prove that the proper risk treatments are selected.

2.7 Instances of Information Security Implemented Policies in UAE

In this section, some of the implemented information security policies in UAE will be explained.

2.7.1 NESA – The New Standard of Information Security in the UAE

The National Electronic Security Authority (NESA), is a governmental body that is responsible for protecting the critical data infrastructure in UAE, and overall improving the cyber security of the nation. In order to accomplish this, NESA has developed a set of protocols, guides, and standard for various government agencies dealing with critical information, and made compliance with them compulsory (Ben Downton, 2015).

2.7.2 Dubai Statistics Corporate Information Security Policy Statement

The Dubai Statistics Centre has recognized that information is critical for business operations and has shown commitment in providing secure information environment to customers, partners, stakeholders, and employees. There are three principles of Information Security in their policy statement, namely; Availability, Confidentiality and Integrity (Dubai Government, 2017).

2.8 Research Conceptual Framework and Hypotheses

Despite the efforts of AD-SDI to push Abu Dhabi governmental entities towards geospatial data sharing, there continues to be a lot of reluctance on the entities' side to comply owing to their perceived risks, their sceptic behavioural attitudes, and their preconceives perceptions about data sharing and the security problems it could entail.

2.8.1 Research Null Hypothesis

The following are null hypothesis formed for developing a security framework for geospatial information data and systems including user attitude, social pressure, and perceived control towards data sharing thereby designing a secure information system:

$H_0$1: Behavioural attitude of users does not influence geospatial data sharing

$H_0$2: Social pressure on users does not influence their intention of geospatial data sharing

$H_0$3: Perceived control factors do not influence users' geospatial data sharing

The above null hypothesis has been examined based on its elements which has been individually dealt by devising sub-hypotheses.

$H_0 1_A$: Beliefs about the implications of geospatial data sharing for an organisation's resources do not influence geospatial data sharing

$H_0 1_B$: Organisational activities to be affected do not influence sharing geospatial data across organisational boundaries

$H_0 1_C$: Strategic position of individual/organisations does not influence attitude towards sharing of geospatial data.

$H_0 1_D$: Moral implications of individual/organisations do not influence attitude towards sharing of geospatial data.

$H_0 2_A$: Expectations of different groups within the GIS community do not influence individual/organisations' intention of geospatial data sharing

$H_0 2_B$: Market pressure by stakeholders does not influence individual/organisations' intention of geospatial data sharing

$H_0 2_C$: Institutional pressure by government and allied agencies does not influence individual/organisations' intention of geospatial data sharing

$H_0 2_D$: Organisational pressure does not influence individual/organisations' intention of geospatial data sharing

$H_0 2_E$: Moral norms do not influence individual/organisations' intention of geospatial data sharing

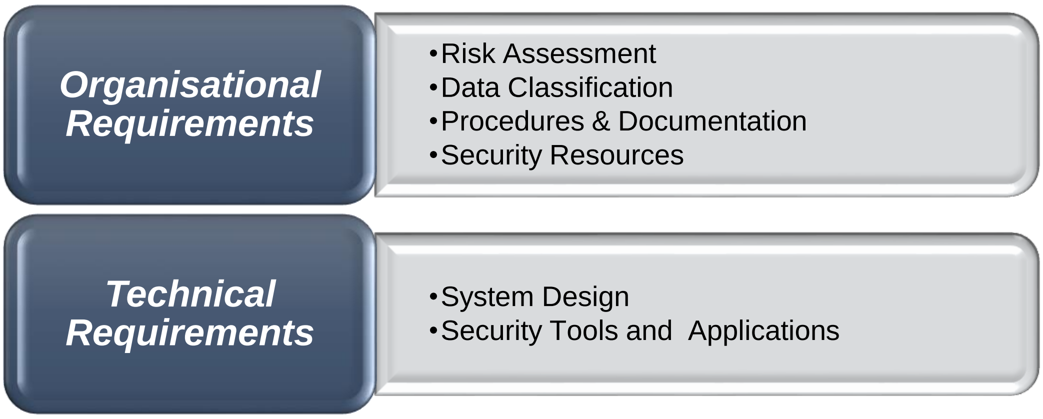
$H_0$3A: Internal perceived control factors do not influence users' geospatial data sharing

$H_0$3B: External perceived control factors do not influence users' geospatial data sharing

2.8.2 Conceptual Framework

A secure information system should maintain anonymity, authenticity, privacy, and security of the sensitive data. For designing such systems, a few criteria must be fulfilled, and they are: appropriate access control mechanism for data access, authentication specification, authorization policies, developing appropriate privacy and trust policies and proper policy specification (including regular risk assessment) for mitigating the risks and threats to geospatial information system.

Based on the above, a conceptual framework was developed for this research study upon exploring the associated elements as depicted below:



Organisational Requirements

- Risk Assessment
- Data Classification
- Procedures & Documentation
- Security Resources

Technical Requirements

- System Design
- Security Tools and Applications

Figure 2-7: The Proposed Conceptual Framework

2.9 Summary of Chapter

This chapter has presented detailed background information on geospatial data and the need for geospatial data security. It provided a review of existing literature on geospatial data security frame work as well as ISMS (Information Security Management Systems) and ISO 27000. The overview on AD-SDI and other information security systems used in UAE is also included. In addition to this, a conceptual framework and hypothesis were proposed.

CHAPTER 3. RESEARCH METHODOLOGY

3.1 Introduction to Chapter

In this chapter, the implementation of the undertaken methodology is explained. The research methodology involves choosing the proper scientific research method to verify and validate the proposed security framework and hypotheses that were presented early in chapter two. To accomplish the purpose, a mixed-method approach is applied, where in the first stage; a survey with different types of users; from common consumers, to government entities using geospatial data, is carried out. The survey provides an understanding of user attitudes towards geospatial information sharing, taking the safety and security aspects of sharing as their main concern. The second stage consists of interviews with representatives from the governmental entities participating in the Abu Dhabi Spatial Data Infrastructure (AD-SDI) to understand their management strategies and the loopholes in the security methodologies that they follow.

Results from both stages of research have provided the input used to develop a customized security framework for protecting geospatial data in Abu Dhabi government. A detailed explanation of each of the methods and tools applied is discussed later in this chapter.

3.1 Gaps in Literature

After reviewing the literature related to the research topic, it has been observed that geospatial data infrastructure methodologies have been vehemently studied over the period of years. Most of the studies included have focused on security frameworks that concentrate on the various access control methods and technical security tools that can be used in them. However, this research has come across a few factors that bring to the light other security aspects related to geospatial data; aspects that do not all revolve around technology. Nonetheless, this research has recognized another research gap in the literature explored, which concludes that none of the studies have studied or proposed a model specifically designed for security of geospatial data in Abu Dhabi.

3.2 Research Design

Research design can be defined as the plan or blueprint for conducting research work, with a focus on data collection that is essential for conducting research in an efficient manner (Newman & Benz, 1998). It also helps in determining the correct path for collecting data from various sources, and analysing data using different methods to interpret the collected information (Blessing et al., 2009). The major parts of research design applied in the study are discussed below.

3.2.1 Research Philosophy

Research philosophy is an effectual tool used in gathering and analysing the data, it also determines the type of data required for a particular research study. According to Kothari (2004), the research philosophy is often defined with respect to the nature of the subject matter, the data required, and the background of research area chosen. Research philosophy is mainly classified into three types, namely; realism (concentrates on the belief of the research topic and its actuality), interpretivism (considered an individualistic approach, that considers the view point of the researcher), and positivism (related to the interpretation made from conducting an investigation in an objective manner) (Kothari 2004). In this research study, Critical Realism based on epistemology objective is used. The critical realism philosophy combines the traditional realism philosophy with social philosophy to develop an interface between the social world and the research work. The epistemology objective is related to objectively experiencing the knowledge related to the topic and not depending on the opinion of others (Britton , 2004).

3.2.2 Types of Data

This study uses both primary and secondary data for accomplishing the work. Primary data collection is used to achieve the aim and objective of the study; and secondary data collection is used to develop the research hypotheses and examine the primary observations made in the initial phase of the study.

3.2.3 Research Method

The research method helps in the understanding of the aims of the research study, and in solving the research problems in the most effective manner possible. Research methods can be classified as exploratory (provides understanding and insight on research problem), descriptive (describes characteristics of the research topic), and explanatory (involves testing applicability and relationships between research variables) (Newman & Benz 1998). This research study uses all three-research methods; the exploratory method is used in this study to explore the in-depth perspective and attitude of AD-SDI representatives towards the security of geospatial data. The descriptive method employed in this study has aided in describing the socio-demographic of users and their general requirements related to geospatial data. In addition to this, the explanatory method is used for understanding the relationship necessary for information sharing over the digital service as well as understanding safety and security aspects concerns of the users.

3.2.4 Research Approach

The research approach is the procedure for collecting and selecting data that can add to the legitimacy and validity of research conducted. Research approaches are classified into a quantitative approach and a qualitative approach. In the quantitative approach, data is collected in numerical form so it can be measured, while in the qualitative approach, data collected is not measurable but is more conceptual in nature and expressed in a descriptive manner (Newman & Benz, 1998). A mixed research approach is used in this study, where both quantitative and qualitative methods are used to form and test the hypothesis.

3.2.5 Research Strategy

The research strategy plays a crucial role in outlining the structure of the research study, and providing a clear picture for the various research techniques used in data collection. The most commonly used research strategies are interviews, case studies, surveys, and experiments (Blessing et al., 2009). In this research, surveys and interviews are used to collect quantitative and qualitative data respectively. Surveys are used in this study to cover a large demographic and vast geographical areas, while interviews are used because they are a direct method of collecting viewpoints of participants. Both methods will work together to provide an understanding of user attitudes towards geospatial information sharing over digital services, taking safety and security aspect into concern.

3.3 Sampling Plan

Sampling is the method by which participants (people or organisations) are selected from the target population for research, so that by studying their answers, the sample's results could be applied more generally to the whole population (Trochim, 2017).

There are two types of sampling methods; non–probability sampling and probability sampling. In probability sampling, all the elements of the population are equi-probable so they have an equal chance of selection, while in non-probability sampling, elements are not equi-probable and have varying chances of selection (Cochran, 1999). The major factors of sampling plan selection are the sample population and sample size. The sample population is the element set that increases effectiveness of the study, and the sample size is the size of sample space or population selected. In the opinion of Teddlie & Yu (2007), a smaller sample size negatively affects the accuracy and reliability of research work whereas a larger sample size consumes more time and cost.

The targeted population includes all the users in AD-SDI entities including both general consumers and government agencies involved.

3.3.1 Sampled Population

Both general users and representatives of government bodies were chosen as the sample population for this research work. The total sample population for the survey was 200; including 120 general users and 80 specialists from four government agencies using geospatial data. Both general users and government representatives were chosen in order to get an overall picture related to the security of geospatial data. The next phase of conducting interviews with representatives of Abu Dhabi Spatial Data Infrastructure (AD-SDI) served to provide an understanding of their IT management strategies and the perceived loopholes in the security framework that could affect geospatial data sharing. For this study, 10 representatives from four governmental agencies were interviewed.

Inclusion Criteria of the sampled population include:

- All respondents are of legal age
- General users have used services for at least a year
- Government representatives must have one year working experience
- Government representatives selected for furthers interviews must have five years of working experience
- All participants in the study must be UAE nationals

Exclusion Criteria of the sampled population includes:

- Under age general users are excluded
- Foreign nationals are not considered
- Interns or representatives with less than required experience are not considered

3.3.2 Research Sampling Plan

In this study, probability cluster sampling is used for selecting survey respondents, and non-probability snowball technique is used for selecting interview participants. In cluster sampling, the population is divided into clusters, and a cluster is selected randomly from all the possibilities, and then a sample is selected randomly from the cluster (Teddlie & Yu, 2007) so it ensures the random selection for survey. Non-probability snowball technique is used so that participants can be selected for further interviews.

3.3.3 Data Collection Procedure

This research has employed both primary and secondary research methodology for this study work. For primary data collection, the quantitative data was collected through surveys with a sample size of 200, and the qualitative data was collected through interviews conducted with 10 government representatives. The research instrument for the survey was a close-ended/structured questionnaire for collecting quantitative data, and for the interview, qualitative data was collected using an open-ended/semi-structured list of questions.

The survey questionnaire is based on a study by Wehn De Montalvo (2004), which was a qualitative study that discussed the effect of behavioural side of users on data sharing with the government of South Africa. The research questionnaire is comprised of sections on general tendencies in using geospatial data and reasons behind it, attitudes towards information sharing over digital services, users' perceptions/awareness on associated risks, and strategies they apply to keep their data safe and secure, followed by a socio-demographic profile. The interview questionnaire includes business & security requirements, risk assessment (assets, vulnerabilities, and threats), risk mitigations and standard controls selections, implementation of controls and security SOP, and monitoring and reviewing (incidents, KPIs, regular review controls, risk reassessment versus changes). Themes involved are access control (role and nature of data), copyrights protection, encryption (media/network), employee awareness, and roles and responsibilities, followed by a socio-demographic profile.

For the secondary data collection, some of sources used to prepare the questions are:

- Journals: Journal of Automation and Information Sciences, Expert Systems with Applications, International Conference on Geoinformatics
- Web-pages: ADSIC and AD-SDI .
- Reports: UN-GGIM, ISO/IEC 27000

3.4 Ethical Considerations

According to Kothari (2004), it is very vital to follow the ethical considerations related to research while conducting any study. As the topic of this research study is information security frameworks for geospatial information, therefore, the chance of affecting the reputation of any enterprise or individual is negligible. While conducting the survey and interviews, an informed consent we taken from every participant in the process. The survey and interviews were not, in any way, imposed on participants, and were only conducted after receiving consent from all the participants.

Prior permissions were also received from respective Human Resource/Employee Welfare departments before initiating the survey upon explaining the study aim and ensuring that data will not be used for anything but this study. Permissions were also sought before conducting the interviews, and prior appointments were set up with respective personal secretaries.

Steps have been taken to abide with the data protection act, and the anonymity of participants in both the survey and interviews was maintained. Participants were informed of the purpose of the study and the significance of their contribution, before recording their responses. All data collected from the secondary sources has been properly cited and referenced, and appropriate recognition was given to sources used. Hence, the research has strictly followed the appropriate research ethics, and proper measures have been taken during the course of research work to maintain the privacy and confidentiality, of respondents' personal and professional data to safeguard them from possible harm and identification.

3.5 Validity and Reliability

For any quantitative research work, validity and reliability are vital parameters to approve and validate the study. The validity is the parameter that establishes whether the research work conducted truly achieves the pre-established aims and objectives, and is a measure of the authenticity of the results obtained from the study. It can also be said that it establishes the extent of success of the chosen research instrument selected for gathering data for the research work. In the opinion of Rogelberg (2002), research work validity can be established by pre-developing the set of research questions and answering them through research work.

The validity parameter of the quantitative research work can be categorized into three categories: First is content validity; which determines whether the research instrument chosen has accomplished all the research objectives. Second is; which is related to the results obtained from data analysis and any inference derived from it. Third is *criteria validity*; which determines whether the chosen research instrument establishes relations between the research variables (Rogelberg 2002). Validity of the quantitative data collected is established through pilot testing 10% of the sampled population and establishing their mean, variance, and variance of equality.

Reliability tests are used to determine the reliability of results obtained by repeating the procedure for a number of times to check its stability with time, it is also related to the *consistency* of the data gathered or measured (Tavakol & Dennick, 2011). The Gaussian distribution or Normal distribution of the data analysed is the basis for most of the statistical operations such as correlation and co-variance. It is often assumed that the samples selected from the sample space will be normally distributed (Rogelberg, 2002). The homogeneity of the work is measured here using Cronbach's alpha method; the most commonly utilized method for testing the homogeneity of selected research instrument (Rogelberg, 2002). It determines how closely related the set of samples are, in order to form group or criteria for internal consistency. The acceptable value is 0.6 and higher to establish inner consistency.

In addition to this, validity and reliability of qualitative data has been maintained through triangulation, to ensure data trustworthiness, rigor and quality. Data triangulation is considered a powerful technique for data validation by cross-verifying it with two or more secondary sources. Particularly, it is related to the study of different research studies, using various research methods.

3.6 Data Analysis Procedure

After the selection of the research topic, reviewing the related literature, developing research hypothesis and framework, choosing research methodology, selecting research design and gathering the required data, the subsequent step has been to scrutinize the gathered data to form the conclusions for this study. Data analysis is an ongoing activity that answers the research questions as well as provides further directions to the data collection process. The main goal of the data analysis procedure is the conversion of raw data into some form of information as well as establishing the link between various data sets. Data analysis of the collected data is a scientific method used in verifying the research hypotheses and framework, and answering the predefined research questions. This procedure is used here for developing accurate results from the quantitative research data collected, as well as understanding the importance and limits of the selected research topic.

The quantitative data collected was first analysed through numerically coding the responses collected from the survey by using MS Excel, and then importing the data to SPSS V21.0. SPSS is a statistical software package, which is generally used for logical data analysis. For descriptive data analysis, frequency distribution is used to compress and summarise the gathered data through grouping and class formation (Thompson, 2009). It is fundamental then to use graphical representation through charts and bar graphs to display data statistics in a comprehensible way.

Another method used for descriptive data analysis is cross tabulation or crosstab method, which allows the understanding of relationships between two variables and observing one-to-many variable relations. It basically tabulates data classes through variable categorizing and comparison (Thompson 2009).

For this research study, the responses obtained from the survey are presented in aggregated form through cross tabulation, that will present data in comprehensible tabular form. For inferential analysis, Pearson correlation and linear regression are applied in this study. The descriptive analysis method is also used in the analysis of the results obtained from the pilot survey conducted using a pilot questionnaire. The results obtained from this analysis were the basis for improvements made in the questionnaire for carrying out the final survey.

3.7 Summary of the Chapter

In this chapter of the study, the research methodology has been properly discussed. The research methods selected for this study have been analysed and appropriate justifications for them have been provided. Additionally, the philosophy of research, research design, research strategy, sample size and methods, methods of data analysis and other elements of the research methodology were discussed in this section. Furthermore, ethical considerations and the tools for ensuring the validity and reliability of research were also included in this chapter.

CHAPTER 4. DATA ANALYSIS AND INTERPRETATION

4.1 Introduction to The Chapter

The purpose of this chapter is to validate the designed hypothesis using quantitative and qualitative analysis of the gathered data through surveys and interviews of governmental representatives working in the geospatial governmental business areas in Abu Dhabi. The quantitative analysis and data processing has been conducted using Statistical Package for Social Science (SPSS - Version 21.0). The entire insights of the quantitative analysis are presented in a form of descriptive and inferential analysis. Additionally, qualitative analysis has been used to collect geospatial representatives' subjective judgments through interviews, providing unquantifiable information such as: representatives' expertise, attitudes, and perceptions.

4.2 Quantitative Analysis

In this study, quantitative analysis has been performed using descriptive and inferential analysis.

4.2.1 Descriptive Analysis

In descriptive analysis, demographic analysis has been performed in order to present the frequency distribution of the demographic variables. Additionally, using frequency distribution, the research has shown whether the organisation's behavioural attitude of government users working in Abu Dhabi government influence geospatial data sharing or not.

4.2.1.1 Demographic Analysis

In this section of the chapter, the analysis will be based on the frequency distribution of the demographic data, and the respondent's data is analysed accordingly.

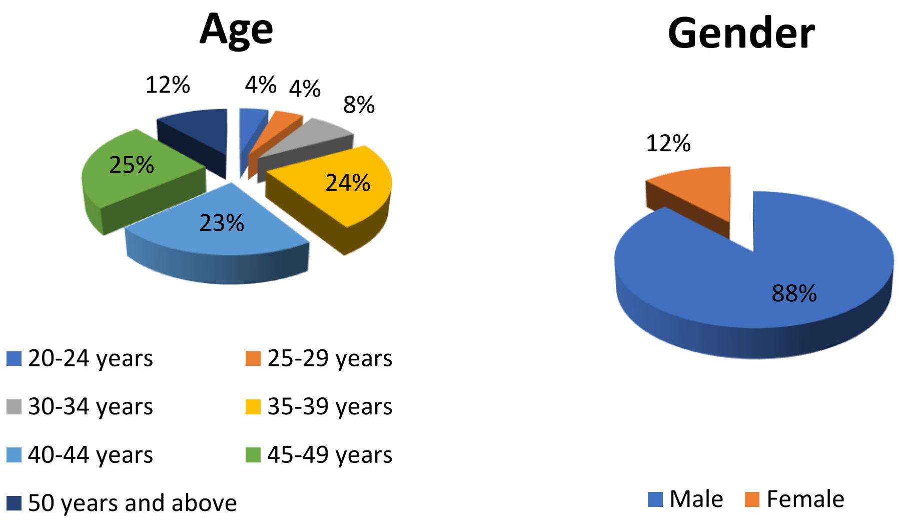


Figure 4-1: Age and gender frequency distribution

Figure 4-1 depicts that people lying under age group 35-50 years constitutes the maximum number of the selected population of working users in Abu Dhabi Government in the business area of geospatial data which is approximately 72%. Also, it has been observed that in comparison with male, female users are relatively less.

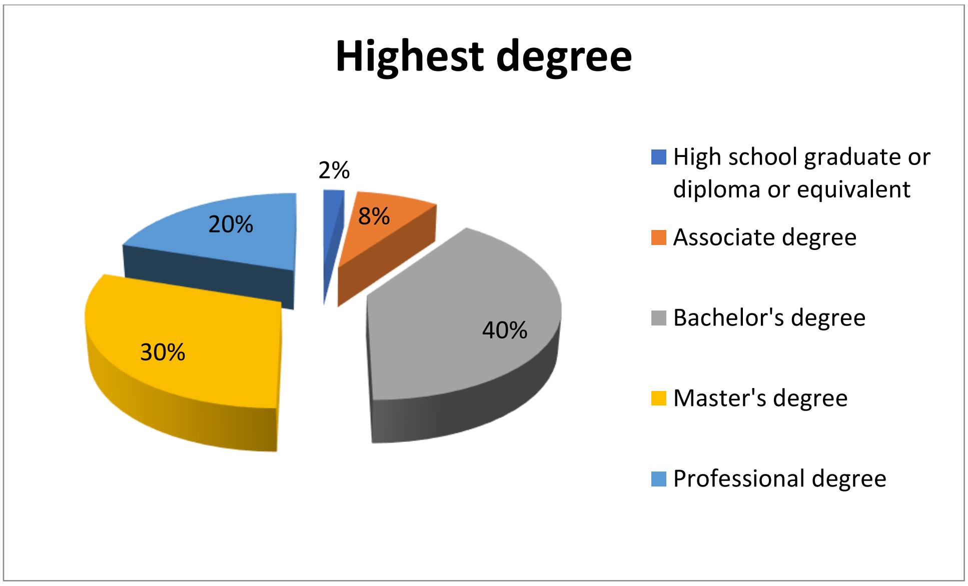


Figure 4-2: Frequency distribution of user's education qualification

The maximum number of respondents in the pool constitutes of graduates and post-graduates, at around 40% and 30% of the population having a graduate degree such as BA, AB, BS, and post-graduate degree such as MA, and MS, respectively.

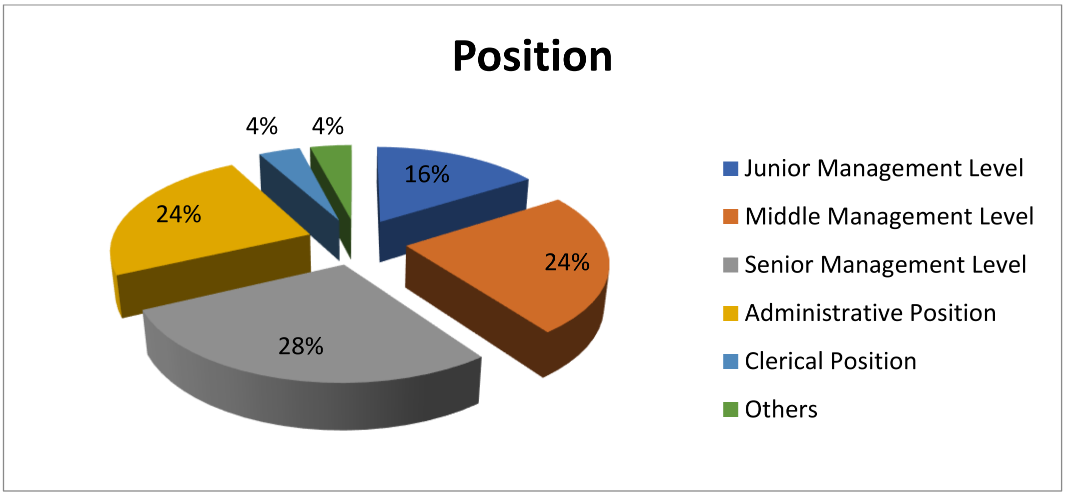


Figure 4-3: Frequency distribution of the users at each level involved in study

The highest number of respondents involved in the study are working on senior management level, followed by users working in administrative positions and middle management levels, followed by users working at junior management levels.

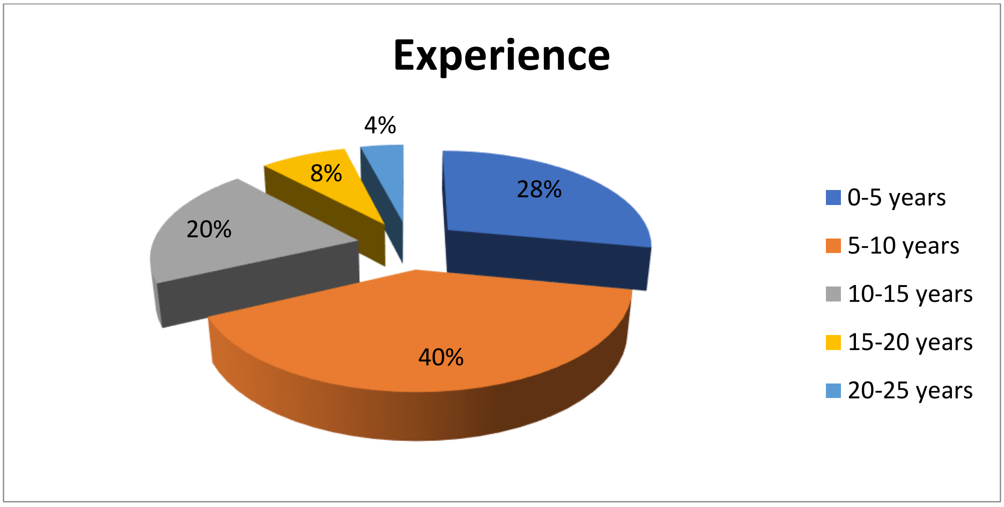


Figure 4-4: Frequency distribution of the experience of the respondents

Most of the respondents involved in study have been with their organisations for a considerable period, with 40% having an experience of 5-10 years, followed by a population of 28% of 0-5 years. Based on the frequency distribution of the demographic variables, it has been identified that the respondents chosen in this study are qualified enough to provide valid information.

4.2.1.2 Behavioural Attitudes of Users and Their Perceptions on Geospatial Data Sharing

This research has examined the behavioural attitudes of users and their perceptions on geospatial data sharing. The behavioural attitude of the users has been measured based on the mean value obtained from the values given by the respondents against each and every statement of the questionnaire; where 1 is the minimum and refers to strongly disagree, and 5 is the maximum and refers to strongly agree.

The questions used in the survey are based on a study by Wehn De Montalvo (2004), that examined the relationship between user's behavioural attitude, strategic position, and the internal and external factor to the environment to the geospatial data sharing behaviour of the organisation.

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
Attitude					
Behavioural beliefs about the resource outcomes					
Time is saved by sharing geospatial data among individuals and entities	200	1	5	3.86	1.323
Effective use of geospatial data sharing can mean that data are collected in the most logical and cost-effective way	200	1	5	3.80	1.349
Need for trained staff for collecting and maintaining new geospatial data is reduced	200	1	5	3.85	1.329
Sharing of geospatial data improves communication and collaboration among different organisations	200	1	5	3.69	1.413
Data storage is saved when cloud storage is used for shared information, so local storage capacity will not be required	200	1	5	3.82	1.315
Introduction of governmental standards act as a motivation for sharing, for once in place, shared data is secure	200	1	5	3.86	1.323
Sharing improves the quality of geospatial data through identification of errors and gaps	200	1	5	3.86	1.323
Behavioural beliefs about the organisational activities					
Sharing of geospatial data help freeing up time and resources to focus on core activity	200	1	5	3.75	1.367
Sharing positively impacts the perceived usefulness of the GIS	200	1	5	3.58	1.444
Sharing geospatial data improves decision-making process in a GIS-using organisation	200	1	5	3.86	1.323

Table 4-1: Users behavioural attitudes on geospatial data sharing

Based on table 4-1, it has been observed that in the context of sharing geospatial data, users in Abu Dhabi Government perceive multiple benefits of data sharing, due to which they tend to share information with other organisations. From table 4-1, it can be concluded that the mean value against all statements is either 4 or tending towards 4, which means that users agree with the statements and consider them major reasons for distribution of geospatial information with other organisations. Additionally, under the category of behavioural beliefs about resource outcomes, users agree that sharing data is time savings, helps in avoiding the need for trained staff, saves data storage, and all other statements in the table are causes of sharing information with others.

Also, the users have agreed that sharing of geospatial data helps in freeing up time and resources to focus on core activities, that sharing positively impacts the perceived usefulness of the Geographic Information System (GIS) data, and improves the decision-making process in a GIS-using organisation, which are all responsible factors for the respondents' data sharing behaviour with other organisation.

4.2.2 Inferential Analysis

This section has been particularly designed to provide an understanding of the impact of organisational strategic positions on geospatial data sharing, along with the impact of external and internal factors on organisation's perceived control on geospatial data sharing.

4.2.2.1 Impact of Strategic Position on The Geospatial Data Sharing

To find out the impact of organisational strategic positions on the geospatial data sharing, initially it was important to find out the correlation between both to understand by what degree they are correlated and the type of correlation between them.

Strategic Position		
		Organisational strategic positions’ influence on geospatial data sharing
Loss of control over data sharing	Pearson Correlation	0.812**
	Sig. (2-tailed)	.000
	N	200
Behavioural beliefs about knowledge creation	Pearson Correlation	0.814**
	Sig. (2-tailed)	.000
	N	200
Normative beliefs about GIS community pressure	Pearson Correlation	.818**
	Sig. (2-tailed)	.000
	N	200
Normative beliefs about market pressure	Pearson Correlation	.757**
	Sig. (2-tailed)	.000
	N	200
Normative beliefs about institutional pressure	Pearson Correlation	.727
	Sig. (2-tailed)	.000
	N	200
Normative beliefs about organisational pressure	Pearson Correlation	.736**
	Sig. (2-tailed)	.000
	N	200
Perceived moral norms	Pearson Correlation	.887**
	Sig. (2-tailed)	.000
	N	200

Table 4-2: Correlation between strategic position and sharing behaviour

From table 4-2, it has been ascertained that all the variables of organisational strategic positions are positively and significantly associated with geospatial data sharing; as by taking the average of sub-factors of individual factors, the correlation range occurred to be 0.727 to 0.887, with significance value less than 0.05. This shows that positive change in variables of strategic position leads to a positive change in geospatial data sharing. Also, the highest association of geospatial data sharing has been found with the variable “perceived moral norms”; with a correlation value r=0.887, and p<0.05. Also, the variable "normative beliefs about Institutional pressure” has been found to be least positively associated with geospatial data sharing; with a correlation value 0.727 and a significance value less than 0.05.

After finding the association between the variables, the research intended to measure the quantity of influence of organisational strategic positions on geospatial data sharing.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.995[a]	.990	.988	.111

Table 4-3: Linear regression model summary

From Table 4-3: Linear regression model summary, based on the value of R^2=0.990 or 99%, it has been determined that organisational strategic positions have a high impact on geospatial data sharing; as organisational strategic positions make a 99% variation in the value of geospatial data sharing. Furthermore, looking at the value of adjusted R^2=0.988, it can be said that if other independent variables are added in the existing list of independent variables, it will not make much difference in the variation explained by the independent variables of the current regression model.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	199.490	31	6.435	523.460	.000[b]
	Residual	2.065	168	.012		
	Total	201.555	199			

Table 4-4: Analysis of variation table to check the significance of the model

Table 4-4 exhibits that the regression model is significant; since the significance value p is less than the standard acceptance level of 0.05. Also, F-value 523.460 of the model shows that the current regression model generates less error in predicting the impact of strategic position on geospatial data sharing.

After determining that organisational strategic positions have a significant impact on geospatial data sharing, the research has proceeded to figure out which of the specified factors of strategic position has how much impact on geospatial data sharing from the table presented in appendix 5.

While looking at appendix 5, all sub-factors of "Loss of Control Over Data Sharing" except sub-factor "Sharing leads to loss of actual use and control of the resource" have been found to have a positive significant impact on geospatial data sharing. Out of 7 sub-factors of “Behavioural beliefs about knowledge creation”, only two of the sub-factors, namely; “Sharing leads to creation of tacit to tacit knowledge” and “Sharing leads to integrated development planning” have no significant impact on the sharing of geospatial data as the significance value is > 0.1, which is the minimum acceptance level for the study. In the same context, the factor “Normative beliefs about GIS community pressure” does not have any significant influence on the sharing of geospatial data; as out of 7, only two sub-factors of it have a significant impact on geospatial data sharing. Also, the factor “Normative beliefs about market pressure” significantly and positively affects geospatial data sharing, since all of its sub-factors except “Commercial spatial data brokers disapprove organisation’s engagement in spatial data sharing” influence geospatial data sharing. Due to the insignificant behaviour of sub-factors of “Normative beliefs about Institutional pressure”, it also does not make any variation in geospatial data sharing. However, the factor “Normative beliefs about organisational pressure” significantly influences geospatial data sharing, since all of its variables except “Mandate (organisational goals/mission) disapprove organisation’s engagement in spatial data sharing” make significant and positive variation in the value of sharing of geospatial data with a significant value < 0.1. Moreover, the factor “Perceived moral norms” has also been found to have a significant role in explaining the variation in geospatial data sharing.

It is noticed that all the variables that have a significant influence on geospatial data sharing have positive impact on it. For instance, the sub-factor “Sharing leads to loss of control of ownership rights or copyrights” in “Loss of Control over Data Sharing” has a significant impact on geospatial data sharing with b=0.106 at significance value <0.05. This shows that a positive change of 1 unit in “Sharing leads to loss of control of ownership rights or copyrights” brings a 10.6% positive change in geospatial data sharing.

Finally, it has been concluded that organisational strategic positions have a significant impact on geospatial data sharing.

4.2.2.2 Impact of Internal and External Factors on Organisation’s Perceived Control on Geospatial Data Sharing

In order to determine the impact of internal and external factors on the perceived control towards geospatial data sharing, the research has again followed the same route, where the degree of association of internal and external factors with organisation’s perceived control on geospatial data sharing has been ascertained. From Appendix 6, it has been observed that internal factors such as “Assessing of quality of spatial data”, “Handling different formats of spatial data”, “Mastering different standards”, and all factors shown in the list of internal factors are significantly and strongly associated with the organisations’ perceived control on geospatial data sharing, where the correlation coefficient r values lie between 0.927 and 0.334. Further, while looking at external factors, it has been observed that all the external factors are also associated with organisations’ perceived control on geospatial data sharing. The range of correlation values for external factors lies between 0.957 and 0.400.

The next step is to determine the impact of the independent variables in “Internal and external factors” on the dependent variable “Organisational perceived control on geospatial data sharing”.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.996[a]	.991	.989	.107

Table 4-5: Model summary of regression model

Table 4-5 shows that the internal and external factors that affect an organisation can lead to a 99.1% variation in the value of organisations’ perceived control on geospatial data sharing.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	204.072	41	4.977	436.185	.000[b]
	Residual	1.803	158	.011		
	Total	205.875	199			

Table 4-6: Analysis of variation table to check the significance of the model

Furthermore, table 4-6 shows that the current regression model is significant in describing the role of independent variables in estimating the values of the dependent variable with a significance value <0.05.

After finding that internal and external variables when combined have significant impact on organisation’s perceived control on geospatial data sharing, the research proceeds to determine the quantitative value of impact of each and every variable of internal and external factor on the dependent variable.

While looking at appendix 7, it has been ascertained that out of 31 internal factors, with the exception of the 12 factors: “Integration of different spatial data sets”, “Usage of metadata interfaces/databases”, “Capturing of metadata”, “Application of metadata”, “Database administration”, “Transfer of spatial data to/from different media”, “Using the internet to distribute spatial data”, “Establishment/fostering of contacts”, “Identification of meeting opportunities”, and “Organisational guidelines”, all other internal factors have a significant impact on organisation’s perceived control on geospatial data sharing; as these variables have a significance value greater than the minimum acceptance level 0.1.

Also, it has been observed that the internal factor “Interpretation of metadata to establish its adequacy determines perceived control on sharing of data” has the highest positive impact with b = 0.488 and significance value <0.1, which means a change of 1 unit in the value of “Interpretation of metadata to establish its adequacy” brings a 48.8% positive change in the value of organisations’ perceived control on geospatial data sharing. Also, there are factors like “Availability of funding”, “Liability agreements”, “Handling different formats of spatial data”, “Mastering different standards”, and “Selection of spatial data for exchange” which negatively influence organisations’ perceived control on geospatial data sharing.

In the case of external factors, factors such as “Compatible purpose of application”, “Organisational fit”, “Policy development”, and “Abu Dhabi core data set identification” have a significant and positive influence on organisations’ perceived control on geospatial data sharing. The factor “Abu Dhabi core data set identification” indicates a high perceived control of organisation on sharing of data with a significance value 0.465, and significance value <0.01. This signifies that a 1-unit change in Abu Dhabi core data set identification increases perceived control on data sharing by 46.5%.

Based on the insights obtained, it can be concluded that both internal and external factors have a significant impact on organisations’ perceived control on geospatial data sharing.

4.2.3 Hypothesis Results

H_01	Behavioural attitudes of users do not influence geospatial data sharing	Reject
H_02	Social pressure on users does not influence their intention of geospatial data sharing	Reject
H_03	Perceived control factors do not influence users’ spatial data sharing	Reject
H_01_A	Beliefs about the implications of spatial data sharing for an organisation's resources do not influence spatial data sharing	Reject
H_01_B	Organisational activities to be affected do not influence sharing spatial data across organisational boundaries	Reject
H_01_C	Strategic positions of individual/organisations do not influence attitude towards sharing of geospatial data	Reject
H_01_D	Moral implications on individual/organisation do not influence attitude towards sharing of geospatial data.	Reject

H_02_A	Expectations of different groups within the GIS community do not influence individual/organisations’ intention of geospatial data sharing	Accept
H_02_B	Market pressure by stakeholders does not influence individual/organisations intention of geospatial data sharing	Reject
H_02_C	Institutional pressure by government and allied agencies does not influence individual/organisations’ intention of geospatial data sharing	Accept
H_02_D	Organisational pressure does not influence individual/organisations’ intention of geospatial data sharing	Reject
H_02_E	Moral norms do not influence individual/organisations’ intention of geospatial data sharing	Reject
H_03A	Internal perceived control factors do not influence users’ spatial data sharing	Reject
H_03B	External perceived control factors do not influence users’ spatial data sharing	Reject

4.3 Gap in Quantitative Analysis

Through quantitative analysis, the research has tried to determine the organisational behavioural attitude and strategic position towards sharing geospatial data information along with the effect of internal and external factors on organisations' perceived control on geospatial data sharing. Nevertheless, it could not identify the role of AD-SDI in data sharing, the challenges faced by AD-SDI in the context of geospatial data sharing, and the strategies used to mitigate the challenges in a detailed way. However, some of the above missing points could be covered by the qualitative analysis.

4.4 Qualitative Analysis

After performing the quantitative analysis, it is required to fill the gap in its results with the information collected from the primary data identified through interviews. While interviewing representatives of AD-SDI community, the research is focused on finding the role of AD-SDI in Geospatial data sharing of organisations, the kind of challenges that AD-SDI members face related to security with other organisations, and the strategies that must be followed to mitigate the risks related to data security of Geospatial data sharing. A total of 10 participants from AD-SDI based on their position and years of experience have been chosen as the potential participants in the context of qualitative information. First, the participants' demographic profile is presented, which is further followed by the thematic analysis of the responses collected through interviews on the basis of the aims and objectives of the research study.

4.4.1 Respondents' Profile

The following table consists of the summarized demographic profile of the participants involved in the study such as name, age, position held, and total years of experience in their current organisations.

Serial No.	Name	Age	Position held	Total Experience (in years) in the post
1.	A	54	Chief Executive	12
2.	B	45	Planning and Strategy Manger	8
3.	C	41	Senior Programmer	6
4.	D	54	Senior Manager on Administrative Level	20
5.	E	45	Junior Manager Administration	7
6.	F	56	Senior Programmer	15
7.	G	55	Senior Manager on Organisational Management Level	24
8.	H	44	System Engineer	12
9.	I	56	Senior Chief Executive	14
10.	J	49	Junior Manager	9

Table 4-7: General information of the participants involved in the study

Table 4-7 clarifies that most of the participants involved in the qualitative study have relevant experience in Geospatial data sharing at governmental entities. Therefore, the participants involved in the study are considered to provide relevant information as per the aim and objective of the study. Also, in order to maintain anonymity and confidentiality, all of the opinions and views about the particular questions from individual participants are in the form of general alphabetical letters throughout the qualitative analysis chapter.

4.4.2 Role of AD-SDI Community in Geospatial Data Sharing of Organisations

In this particular section of the study, the focus is on finding the role of AD-SDI in covering the geospatial data standard, how the standard benefits the GIS community of Abu Dhabi, and how pragmatic AD-SDI is in developing the standard to accommodate newer demands.

For the question asked about “The role of AD-SDI in coverage of geospatial data standards”, participants A, B, E, G, and H shared that AD-SDI oversees governmental data sharing of Abu Dhabi government among different entities. Participant A clarified it through an example: In case Abu Dhabi Water and Electricity Authority (ADWEA) requires data regarding the transportation network which is hosted by the Transportation Department of the city, then AD-SDI works as the hub of providing that data. Also, participants C, D, and I mentioned that AD-SDI addresses the technical and institutional aspects of gathering, organizing, analysing, presenting, distributing, merging, and maintaining the geospatial data, in order to make the sharing of Geospatial data smooth among the stakeholder community.

Further, participant J added that while AD-SDI oversees the management of Geospatial data, it individually addresses the vital standards for information security. In regards to the question asked “In what way does this standard benefit the GIS community of Abu Dhabi?”, participants A, C, D, E, H, and I mention that the standards remove the barriers in exchanging and sharing information among dissimilar systems, improve the quality of data and configuration management which further enhances users’ confidence, provide a broader range of geospatial data, integrate the systems by enabling the use of data across a broader spectrum of applications, reduce data duplications along with data collection costs, and increase the number of public users.

Participants B and F added that AD-SDI standards’ coverage has raised data exchanging among government institutions by providing access to data sources with a minimum level of hindrances, improved consistency, data interoperability, data security, cross-jurisdictional decision making, and has also helped in reducing the risk and cost of innovation. Other participants of the study also added that the AD-SDI standards coverage has given some supplementary benefits such as: the enhanced ability of re-using data, less data collection redundancy, transparent methods of data collection and processing, benefits to the organisation and community, and better funding opportunities.

With respect to the question "How pragmatic is the AD-SDI in developing the standard to accommodate newer demands?", participants replied that they are meeting the new objective of achieving optimal utilization and reducing duplication of the geospatial data in their geospatial program. Furthermore, it was highlighted that there is a new infrastructure tool named Facility Locator that enables the entities to locate their related facilities on an interactive map through configuration and very limited requirements of geospatial related knowledge. Also, the AD-SDI program provides consulting services and guidelines that give assistance to support businesses and it focuses on the advancement of infrastructure tools and methods which support transformation process in the governmental e-services. Thus, AD-SDI has gained the support of various stakeholders due to its pragmatic behaviour in accommodating newer demands.

4.4.3 Challenges Related to Data Security

While users share geospatial information, security is the major challenge that can result in various negative effects on the image of AD-SDI's entities and users. This section details the challenges faced by AD-SDI while managing information with government entities.

First, when asked the question "AD-SDI in its charter mentions the significance of security and lists it as one of the standard's benefits. Still, there are lingering issues of information security. Why?", six of the participants, namely; A, C, D, E, F, and H replied that the lack of information security personnel in entities to carry out the required security operational process. Further, B, G, and I added that the issues related to information security of geospatial data is due to the undefined responsibilities of security officers. Their roles and responsibilities' matrix should be defined to them as it can help in identifying the level of accessibility of data. Also, respondent J argued that data is not always shared as per the standards of the organisation, therefore, in order to refrain from the occurrence of security issues the data must first be classified according to the classification standards of the organisation.

Additionally, moving next in the challenges section, interviewees were asked "Do you think infrastructure-related vulnerabilities affect the security of information shared? Are there any cases as such experienced by you?" Regarding this question, all participants responded that copying classified datasets on unencrypted transfer media due to inadequate copying policies. However, mutual efforts of AD-SDI entities and ADSIC led to the rate of these incidents falling by a considerable amount.

While exploring the challenges in the last section, another question was asked "Are there any risks related to the sensitivity classification of data? If so, how do you address them?" With respect to this question, participants A, B, C, and E agreed that there sometimes are risks related to problems with the classification of sensitive data. Inappropriate handling of data and information results in security threats from unauthorized access; such as: harm to reputation, identity theft, financial losses, privacy takeover, and others. In this context, participants D, G, and H said that sharing data with unauthorized entities or individuals is a big risk because of the lack in classification standards. Tending towards the way they address it all participant agreed that data classification standards must be set clearly based on the level of sensitivity of the datasets and information assets to ensure the availability of data only to the people who have authorized access to it. For instance, datasets must be classified respective of risk of unauthorized access based on the category they fall in, such as: Secret, Confidential, For Official Use Only (FOUO), and Public. Additionally, in order to avoid uncertain or certain incidents, the classification of sensitive data must be reviewed quarterly, monthly, and weekly. For instance, medium level risk data requires a review quarterly, while high level risk data needs attention within the current financial year monthly, and more urgently, data under very high risk requires immediate attention from management with reprioritization of resources as necessary.

4.4.4 Strategies to Mitigate Geospatial Data Security Risks

To mitigate the identified security threats in sharing geospatial data, some strategies need to be followed by the representatives of the organisation. In the same context, questions were raised regarding the strategies chosen by governmental authorities such as: "What are the core strategies associated with the security of risk assessment?". To that, seven out of ten respondents replied that risks are assessed using five-step process: Establish a risk management framework, identify risks, analyse risks (impact and likelihood), Evaluate risks, and Select risk treatment options. After this, the assessed risks are managed through the PDCA (Plan-Do-Check-Act) model. Using this model, management identifies which type of the control is needed and at which time. This model also helps implement the appropriate security controls so all risks can be handled. This model includes risk assessment, information security design, security testing, and certification and accreditation. While agreeing with the statements of all 7 participants, the rest of the respondents added that the controls defined for each type of risk are taken into use to mitigate threats.

In the same context, interviewees were asked the question: “What are the risk management policies you follow to mitigate existing and potential challenges? And to what extent does that help you in the accuracy of prediction?” To this question, 5 of the participants, namely; A, C, D, F and I replied that in order to manage risks, different strategies like: avoidance, acceptance, transference, and mitigation are followed. If they feel some kind of threat that can be avoided, they tend to remove the source of threat. For instance, re-engineering the business process to remove the source of threat. Agreeing with this, participants B, G, and J further added that whereas, some of the risks that are not quite sensitive are accepted and addressed later on, some of which are addressed by transfer; such as financial risks which are addressed by transferring the financial responsibility to insurance companies via acquisition of insurance coverage. However, they noted that in that case, business would be impacted anyway. Participants E and G also nodded in acceptance of the fact discussed by other participants, and further said that in order to lessen the impact of any risk which cannot be stopped, they apply some intervention such as security monitoring. Further, the question was raised: “In what ways do you ensure a secure design system by addressing potential challenges?”. Participants A, B, C, E, F, G, and I replied that to ensure their security system they check security through working with the 12 domains of standard security; information security of governance, risk management, security of human resource, third party supplier and physical and environment, providing training, managing information assets, designing and testing information system, managing and identifying access to information system, information security of operations, incidents, and continuity management. The remaining participants added that all of these 12 domains are closely assessed time after time to ensure the security of design systems. Further on the question, “Do you think collaboration among organisations ensure a faster remedy? How?”, all participant showed a positive response by stating that indeed collaboration among organisations work faster as a remedy. For instance, through their program, AD-SDI is empowering government as well as society through providing open access to excellent quality and updated geographic data information. Further, it helps in information exchange, promoting and supporting the policies and government regulations for data sharing. Also, ADSIC is working as a centre point of distributing data to other organisation for their ease. Thus, collaboration among the organisations is surely a faster remedy.

Following the same trend, participants were asked to “State some future scope of development in terms of information security maintenance of geospatial data”. On this, the participants replied that under the risk management policy of Abu Dhabi to keep the information and its sharing secure, all governmental entities are required to be certified and accredited under ISO/IEC 27001. In the case of lack of certification and accreditation, it cannot be ensured that the controls and roles and responsibilities of entities and every user involved in the security system has been defined clearly. Also, entities or users would not be considered to work effectively, which could be a major cause of information breaches in the system that needs to be addressed. Other than this, the risk management process is reviewed once in three years, until and unless any major security threats occur. The participants further added that reuse and integration benefits bring technical inconsistencies and non-technical issues, belonging to social, institutional, jurisdictional, legal, and political realms of the organisations. Furthermore, the participants added that the lack of coordination between government organisations and agencies, between managers and technical staff due to their level of understanding of the implementation of whole process, and the communication gap between IT staff and decision makers of geospatial business areas could have huge implications in terms of security. Additionally, participants said that they have faced issues related to data acquisition, data integration, and the lack of standardisation and encryption tools.

4.5 Summary of The Chapter

In this chapter, the research has presented the quantitative and qualitative analysis in detail, examining the information collected through surveys and interviews with representatives of the geospatial data community in Abu Dhabi government that show their attitudes, perceptions, and opinions about geospatial data sharing and its relationship to information security and perceived risks to it. Following this chapter, the next chapter is formulated to provide this study with a conclusion, along with recommended solutions to the problems that have been presented.

CHAPTER 5. CONCLUSION

5.1 Introduction to Chapter

In this current chapter of the study the research has presented the conclusion which has been derived based on the findings of analysis. This particular chapter of the study has been fragmented into the following parts:

- Discussion of research questions which provide more close insights on the risk assessment, attitudes and perceptions of users and representatives of geospatial data community
- Recommendation to Abu Dhabi government entities that work with geospatial data security
- And a summary of the study along with future scope and limitation of the study

5.2 Discussion of Research Questions

Based on the literature review, along with the information collected from the survey and interviews, answers to the research questions posed earlier could be furnished as follows:

Can security applications and technology be sufficient to overcome security challenges in the context of geospatial information and geospatial data sharing? What other areas can we look into?

Based on the research results, the shortcomings of security applications and technology have proven to be very clear, as they, alone, do not provide governmental entities or their users with the required security to share their data with other entities or make their information securely accessible outside of their own entity. Hence, the conceptual model suggested in the literature review chapter of this research has proven useful, as it provides governmental entities with a number of organisational security requirements that add many layers of protection and security to supplement the technical requirements of a secure geospatial data system as shown in Figure *5-1* below.

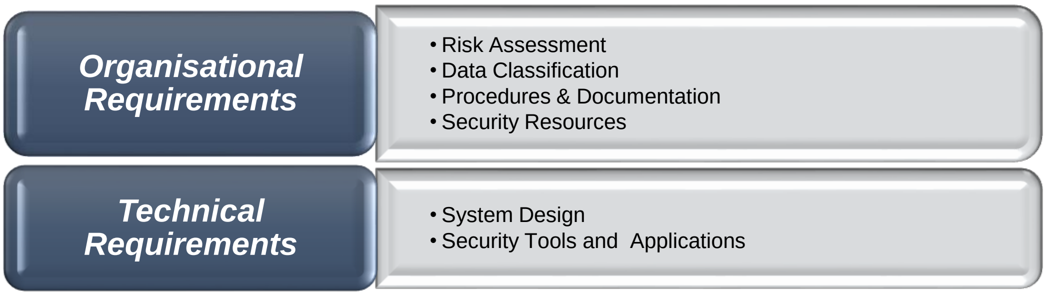


Figure 5-1: Conceptual Framework of Geospatial Information Security

In the conceptual model above, the organisational requirements include: Risk Assessment; that provides the necessary process for risk identification, analysis, and treatment, Data Classification; which enforces the importance of proper data classification according to organisational standards, the use of employees' roles and responsibilities to identify their access rights to different levels of sensitive information, and the periodic reviews of the classifications and access rights associated to them, Procedures and Documentation; which includes the different standards, guidelines, and agreements to be followed, the different accreditations and certifications to be awarded, along with the different contracts, copyrights, and ownership rights to be honoured, and finally, Security Resources; that includes the need for qualified and trained security personnel, with properly defined roles and responsibilities, sufficient budget, and open communication channels with decision makers in higher management. The breakdown of these requirements is shown in Figure *5-2* below:

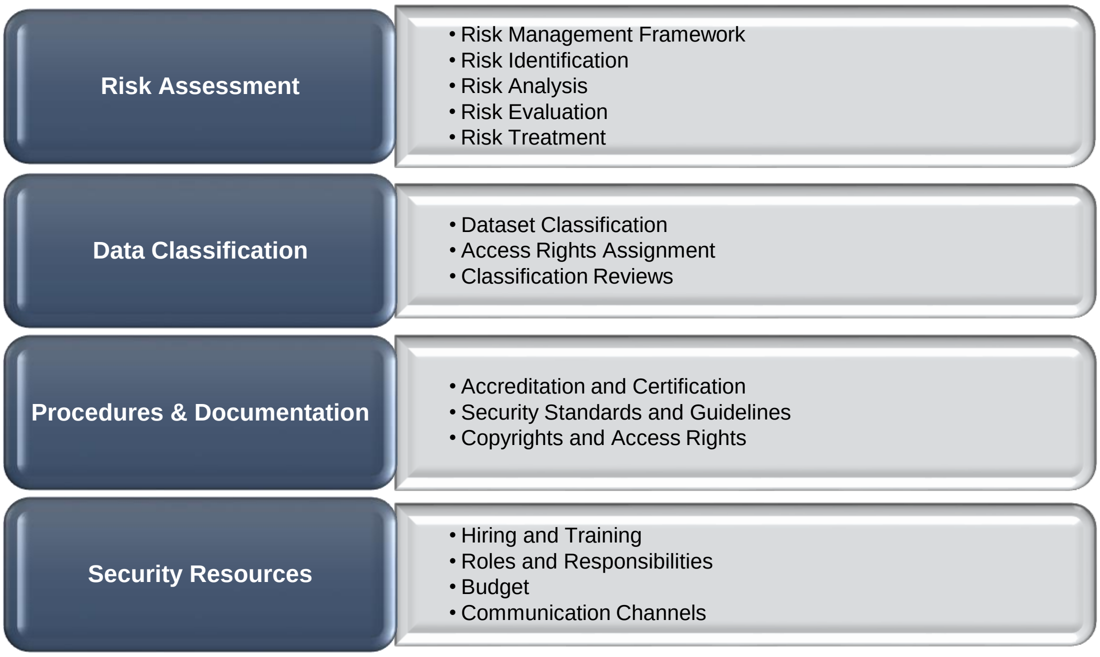


Figure 5-2: A Breakdown of The Organisational Requirements of The Suggested Geospatial Information Security Conceptual Framework

That being said, the technical requirements of a secure geospatial information framework are not to be neglected. Hence, in the suggested conceptual framework, Technical Requirements are the second section of the model, including two sub-sections; System Design and Tools and Applications. The breakdown of these requirements is shown in (Figure 5-3) below:

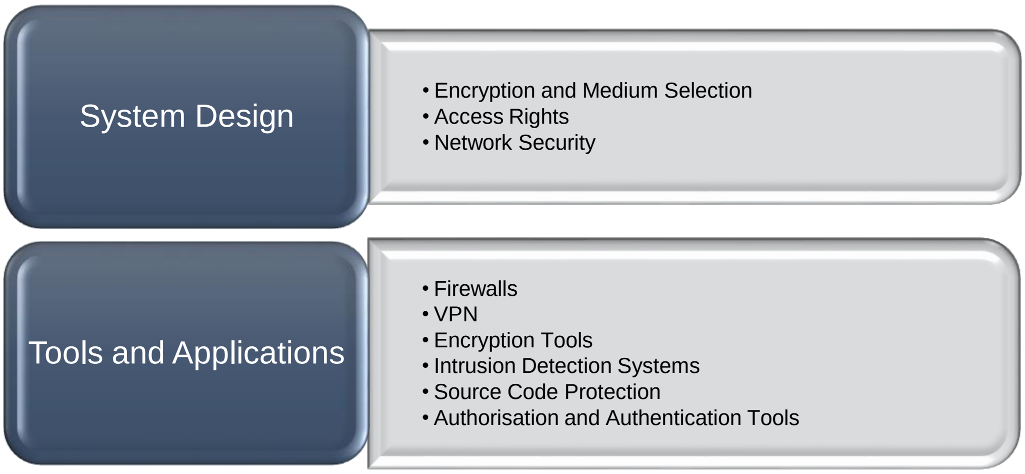


Figure 5-3: A Breakdown of The Technical Requirements of The Suggested Geospatial Information Security Conceptual Framework

That being said, it is concluded that only by fulfilling both technical and organisational requirements in a geospatial information system framework can it be secure enough for users and governmental entities to have the confidence to share data with other entities.

What is the role of users' behavioural attitudes, strategic positions and perceptions, and internal and external control factors on geospatial data sharing in the context of security?

While doing quantitative analysis of the study, the crucial impact of user's behavioural attitude, strategic positions, and the internal and external factor to the environment has been clearly identified. It has been observed that if the organisation has skilled employees who can manage the security of data well, sharing the geospatial data will help them in reducing the time, extra efforts of employees. Also, AD-SDI entities feel that sharing information with others helps them in improving the quality of the collected data through comparison and the identification of errors in the data, as well as help in managing the storage capacity of information as sharing reduce the storage burden. It was also clear that employees felt that sharing data also benefits the organisation in taking effective decisions.

As for users' strategic positions influence on their geospatial data sharing behaviour, some participants feel that sharing data with multiple users may make them lose control over their data. However, a number of respondents believe that sharing data tends to create more knowledge and improve organisational relationships, which influences data sharing behaviour positively. Further, market and organisational pressure, perceived norms, as well as external and internal factors also have an impact on geospatial data sharing behaviour of individuals.

It is worth mentioning that the findings of this research survey are in line with the study by Wehn De Montalvo (2004) on which the survey was based, as both show that users' behavioural attitudes, strategic positions, and environmental factors affect geospatial data sharing behaviour in the organisation.

That being said, although attitudes, strategic positions, perceptions, and different environmental factors cannot be altered overnight, the implementation of the conceptual framework for geospatial information suggested in the literature review can significantly help reassure users that information can still be safe if shared using the appropriate channels, with the appropriately authenticated and accredited entities, and in accordance with the appropriate data classifications, access rights, and standards.

How can the process followed to assess and treat the risks associated with geospatial data in AD-SDI help encourage users and entities to embrace geospatial data sharing?

In order to secure the sensitive geospatial information of governmental entities and its lifecycle at all the places where data is processed, risk assessment is needed. Risk assessment allows the governmental entities to get an accurate image of the threats to geospatial data, so they can support their e-government services and data sharing. This image takes into account the assets that genuinely require protection, as well as the impacts and likelihoods of potential threats, and then it helps in the decision-making process, so effective treatments of the risk can be selected. Enforcing and monitoring the information is the shared responsibility of each governmental entity's Chief Information Security Officer (CISO), and Accountability Authority of Abu Dhabi.

Risk Assessment process in ISO 27001 is made up of five different steps namely; Establishing a risk management framework, identifying risks, analysing risks (Impact and Likelihood), Evaluating risks, and Selecting risk treatment strategies. If this process is applied properly, a lot of risks will be identified and treated before they can cause any damage, and with that confidence, governmental entities will have less reasons to fear security breaches in relation to geospatial data sharing, and they would be more likely to share data with other entities.

How can data classification as well as related users' access rights affect perceived security issues in the context of geospatial data sharing?

Based on the results collected in the analysis chapter of this study, it is clear that proper classification of geospatial data based on its sensitivity, and the access rights granted to different employees in an organisation have a huge impact on how users of data feel about data sharing, especially with regards to security issues. Hence, if proper classification of data in the organisation is done, in line with the governmental standards; dictating which data is secret, confidential, for official use only, or public, and if meticulous precautions were taken in giving access rights to data to personnel based on their job roles and responsibilities, while taking care to periodically review those classifications and access rights, users would feel that only appropriately cleared personnel would have access to sensitive data, and would be a lot more likely to share this data.

5.3 Recommendations to Governmental Entities in The Context of Geospatial Data Security

Based on the findings of the analysis carried out in the previous chapter, and the research questions discussed in this chapter, the research has found some loopholes which need to be taken care of to reduce threats, vulnerabilities, and thereby information security risks. For this, the following recommendations are offered:

- The implementation of the suggested geospatial data system security framework introduced in the study
- AD-SDI entities should strengthen actions in terms of geospatial information sharing on organisations who do not adhere to the risk assessment process, especially with those who are not certified and accredited under ISO/IEC 27001 standards.
- Proper Classification of data needs to be applied to all data sets, and access rights to this data need to be given to users based on their job's roles and responsibilities, with periodic review of both the classification and the access rights.
- Following organisational and international standards, regulations, and guidelines of security, as well as pursuing the proper certifications and accreditations such as ISO 27001.

- Hiring and training of skilled security officers and personnel in the organisation, and assigning them clear roles and responsibilities, with sufficient budgets and communication channels with decision makers
- Collaborating with private organisations that have attained high proficiency in secure system design to benefit from their expertise.
- Conducting training programs for enhancing the employee’s understanding of the benefits and conditions of secure data sharing.

5.4 Summary and Recommendations for Future Scope

While reviewing the study, it has been noticed that Abu Dhabi governmental entities are working effectively in regulating geospatial data within the government and with private entities. Although diligent effort was put into collecting information and establishing the findings of the study, the area still needs future work, as the study has mostly focused on certain aspects such as geospatial data sharing and information security. Future researchers may replicate the suggested model in other organisations, public and private, in UAE and internationally. Furthermore, they can explore other challenges that prevent users of geospatial data from sharing information in contexts other than security issues.

REFERENCES

ADSIC, 2013. [online] Available at: https://www.abudhabi.ae/cs/groups/public/documents/attachment/mtmz/njg0/~edisp/adsic_nd_133684_en.pdf [Accessed 13 Oct. 2017].

AD-SDI, AD-SDI Standards Coverage.

Bernard, R., 2007. Information Lifecycle Security Risk Assessment: A tool for closing security gaps. *Computers & Security*, 26(1), pp.26–30.

Bertino, E., Thuraisingham, B., Gertz, M. and Damiani, M.L., 2008, November. Security and privacy for geospatial data: concepts and research directions. In *Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS* (pp. 6-19). ACM.

Blessing, L.T. and Chakrabarti, A., 2009. *DRM, a design research methodology*. Springer Science & Business Media.

Boxall, J., 2005. The nature of geospatial information and security. *Government Information Quarterly*, 22(4), pp.644–662.

BRITTON, R., 2004. SUBJECTIVITY, OBJECTIVITY, AND TRIANGULAR SPACE. *The Psychoanalytic Quarterly*, LXXIII(1), pp.47–61.

Cochran, W.G. (William G., 1999. *Sampling techniques*, Wiley.

Disterer, G., 2013. ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 04(02), pp.92–100.

Ben Downton, 2015. NESA – The New Standard of Information Security in the UAE.

FGDC, 2005. Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns.

GAO, 1999. Information Security Risk Assessment, Practices of Leading Organisations, Geospatial World, 2010. Abu Dhabi Pioneers a Collaborative Approach to Sharing and Utilizing Geospatial Data - Geospatial World.

Dubai Government (2017). *Corporate Information Security Policy Statement*. [online] Dsc.gov.ae. Available at: https://www.dsc.gov.ae/en-us/About-Us/Pages/Corporate-Information-Security-Policy-Statement.aspx [Accessed 13 Oct. 2017].

IRQS, 2013. Information Security Management System.

Itgovernance.co.uk. (2017). *ISO 27001 Risk Assessments*. [online] Available at: https://www.itgovernance.co.uk/iso27001/iso27001-risk-assessment [Accessed 24 Oct. 2017].

Karabacak, B. & Sogukpinar, I., 2005. ISRAM: information security risk analysis method. *Computers & Security*, 24(2), pp.147–159.

Kothari, C.R., 2004. *Research methodology : methods &amp; techniques*, New Age International (P) Ltd.

Kussul, N.N. et al., 2010. Disaster Risk Assessment Based on Heterogeneous Geospatial Information. *Journal of Automation and Information Sciences*, 42(12), pp.32–45.

Lo, C.-C. & Chen, W.-J., 2012. A hybrid information security risk assessment procedure considering interdependences between controls. *Expert Systems with Applications*, 39(1), pp.247–257.

Mathworks.com. (2017). *What Is Geospatial Data? - MATLAB & Simulink - MathWorks United Kingdom*. [online] Available at: https://www.mathworks.com/help/map/what-is-geospatial-data.html [Accessed 13 Oct. 2017].

Ma, F. et al., 2010. The fine-grained security access control of spatial data. In *2010 18th International Conference on Geoinformatics*. IEEE, pp. 1–4.

Mishra, A.K. & Coulibaly, P., 2009. Developments in hydrometric network design: A review. *Reviews of Geophysics*, 47(2), p.RG2001.

Newman, I. & Benz, C.R., 1998. Qualitative-quantitative Research Methodology: Exploring the Interactive Continuum, SIU Press.

Orlandini, R., LibGuides: Geospatial Data: What is Geospatial Data?

Rogelberg, S.G., 2002. Handbook of research methods in industrial and organisational psychology, Blackwell Publishers.

Schäffer, B., Authentication and Authorization in Spatial Data Infrastructures.

Shekhar, S. et al., 2002. Spatial Contextual Classification and Prediction Models for Mining Geospatial Data. *IEEE TRANSACTIONS ON MULTIMEDIA*, 4(2).

Systems and Information Centre (2017). [online] Available at: https://adsic.abudhabi.ae [Accessed 13 Oct. 2017].

Tavakol, M. & Dennick, R., 2011. Making sense of Cronbach's alpha. *International Journal of Medical Education*, 2, pp.53–55. Available at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4205511/ [Accessed July 10, 2014].

Teddlie, C. & Yu, F., 2007. Mixed Methods Sampling. *Journal of Mixed Methods Research*, 1(1), pp.77–100.

Thompson, C.B., 2009. Descriptive Data Analysis. *Air Medical Journal*, 28(2), pp.56–59.

Trochim, W. (2017). *Sampling*. [online] Socialresearchmethods.net. Available at: https://www.socialresearchmethods.net/kb/sampling.php [Accessed 24 Oct. 2017].

UN-GGIM, 2016. Abu Dhabi Spatial Data Infrastructure (AD-SDI).

Wang, L.G. and Wang, Z., 2006. Spatial information security in geographic information system based on RBAC. Geospatial Information, 4(4), pp.22-24.

Wehn De Montalvo, U., 2004. Mapping the determinants of spatial data sharing. , pp.1–31.

Zarki, M. El et al., Security Issues in a Future Vehicular Network.

Zhang Yanqun & Wang Qianping, 2008. Security Model for Distributed GIS Spatial Data. In *2008 International Symposium on Information Science and Engineering*. IEEE, pp. 641–645.

Zope-Chaudhari, S. and Venkatachalam, P., 2013. Conceptual framework for geospatial data security. International Journal of Database Management Systems, 5(5), p.29.

APPENDIX 1: QUANTITATIVE QUESTIONNAIRE

Section A: Behavioural Attitude of Users and Their Perception on Geospatial Data Sharing

The following questions are based on based on 5-point Likert scale with 5 denoting strongly agree and 1 = strongly disagree, with 3 being neutral.

	5	4	3	2	1
Attitude					
Behavioural beliefs about resource outcomes					
Time is saved by sharing geospatial data among individuals and entities					
Effective use of geospatial data sharing can mean that data are collected in the most logical and cost-effective way					
Need for trained staff for collecting and maintaining new geospatial data is reduced					
Sharing of geospatial data improves communication and collaboration among different organisations					
Data storage is saved when cloud storage is used for shared information, so local storage capacity will not be required					
Introduction of governmental standards act as a motivation for sharing, for once in place, shared data is secure					
Sharing improves the quality of geospatial data through identification of errors and gaps					
Behavioural beliefs about the organisational activities					
Sharing of geospatial data help freeing up time and resources to focus on core activity					
Sharing positively impacts the perceived usefulness of the GIS					
Sharing geospatial data improves decision-making process in a GIS-using organisation					

1. Do you think the organisation's behavioural attitude influences geospatial data sharing?

□ Strongly Disagree

□ Disagree

- □ Undecided
- □ Agree
- □ Strongly Agree

Section B: Strategic Position of Users and Their Perception on Geospatial Data Sharing

The following questions are based on based on 5-point Likert scale with 5 denoting strongly agree and 1 = strongly disagree, with 3 being neutral.

Strategic position					
Loss of Control over Data Sharing	5	4	3	2	1
Sharing leads to loss of control of ownership rights or copyrights					
Sharing leads to regulated access without necessarily owning the resource					
Sharing leads to loss of actual use and control of the resource					
Sharing leads to loss of the ability to rule or regulate possession, allocation and use of the resource and enforcement of legislation					
Behavioural beliefs about knowledge creation *** "** **Tacit knowledge** is the kind of **knowledge** that is difficult to transfer to another person by means of writing it down or verbalizing it" *** "** **Explicit knowledge** is **knowledge** that can be readily articulated, codified, accessed and verbalized. It can be easily transmitted to others. Most forms of **explicit knowledge** can be stored in certain media. The information contained in encyclopaedias and textbooks are good examples of **explicit knowledge**"					
Sharing leads to creation of explicit to explicit knowledge					
Sharing leads to creation of explicit to tacit knowledge					
Sharing leads to creation of tacit to tacit knowledge					
Sharing leads to creation of tacit to explicit knowledge					
Sharing leads to Inter-organisational relationships in terms of redistribution of relative power and influence in organisational environment					
Sharing leads to integrated development planning					
Sharing leads to distribution of benefits to society at large					

*Definitions of tacit and explicit knowledge from Wikipedia.com

Normative beliefs about GIS community pressure					
Local governmental authorities' GIS users disapprove the organisation's engagement in spatial data sharing					
GIS users of federal government disapprove the organisation's engagement in spatial data sharing					
Municipal GIS users disapprove the organisation's engagement in spatial data sharing					
Parastatal organisations' GIS departments disapprove the organisation's engagement in spatial data sharing					
Private sector GIS users disapprove the organisation's engagement in spatial data sharing					
Non-Government Organisation (NGO) GIS users disapprove the organisation's engagement in spatial data sharing					
Academic research institutions' GIS users disapprove the organisation's engagement in spatial data sharing					
Normative beliefs about Market pressure					
Commercial spatial data brokers disapprove organisation's engagement in spatial data sharing					
Public spatial data providers disapprove organisation's engagement in spatial data sharing					
Private spatial data providers disapprove organisation's engagement in spatial data sharing					
GIS suppliers disapprove organisation's engagement in spatial data sharing					
Normative beliefs about Institutional pressure					
AD-SDI disapprove organisation's engagement in spatial data sharing					
Spatial data agreements disapprove organisation's engagement in spatial data sharing					

Politicians disapprove organisation’s engagement in spatial data sharing					
Normative beliefs about organisational pressure					
Other departments within same organisation disapprove organisation’s engagement in spatial data sharing					
Management of the organisation disapprove organisation’s engagement in spatial data sharing					
Individual champions for sharing disapprove organisation’s engagement in spatial data sharing					
Mandate (organisational goals/mission) disapprove organisation’s engagement in spatial data sharing					
Perceived moral norms					
Sharing is perceived as an obligation for the sake of integrated development planning					
Sharing is perceived as an obligation for the sake of society at large					

2. Do you think the organisation’s strategic position influences its geospatial data sharing?

□ Strongly Disagree

□ Disagree

□ Undecided

□ Agree

□ Strongly Agree

Section C: Perceived Control Over Geospatial Data Sharing

The following questions are based on based on 5-point Likert scale with 5 denoting strongly agree and 1 = strongly disagree, with 3 being neutral.

Internal Factors	5	4	3	2	1
Assessing of quality of spatial data determines perceived control on sharing of data					

Handling different formats of spatial data determines perceived control on sharing of data					
Mastering different standards determines perceived control on sharing of data					
Selection of spatial data for exchange determines perceived control on sharing of data					
Integration of different spatial data sets determines perceived control on sharing of data					
Interpretation of metadata to establish its adequacy determines perceived control on sharing of data					
Usage of metadata interfaces /databases determines perceived control on sharing of data					
Capturing of metadata determines perceived control on sharing of data					
Application of metadata standards determines perceived control on sharing of data					
Maintenance/updating of metadata of metadata standard determines perceived control on sharing of data					
Database administration determines perceived control on sharing of data					
Using the internet to locate spatial data source determines perceived control on sharing of data					
Using the internet to distribute spatial data determines perceived control on sharing of data					
Transfer of spatial data to/from different media determines perceived control on sharing of data					
Establishment/fostering of contacts determines perceived control on sharing of data					
Identification of meeting opportunities determines perceived control on sharing of data					
Collaboration with other determines perceived control on sharing of data					
Multi-disciplinary teamwork determines perceived control on sharing of data					
Pricing of spatial data determines perceived control on sharing of data					
Data ownership agreement determines perceived control on sharing of data					

Liability agreements determines perceived control on sharing of data					
Bad experiences with spatial data sharing with other organisations determines perceived control on sharing of data					
Clear overview of the consequences of spatial data sharing with other organisations determines perceived control on sharing of data					
Sufficient Staff determines perceived control on sharing of data					
Availability of funding determines perceived control on sharing of data					
Organisational guidelines determine perceived control on sharing of data					
Control beliefs about dependence on spatial data					
Importance of spatial data to own organisation determines perceived control on sharing of data					
Copyright determines perceived control on sharing of data					
Regulated access determines perceived control on sharing of data					
Availability of alternative sources determines perceived control on sharing of data					
Stability of alternative sources determines perceived control on sharing of data					
Spatial data self-sufficiency of the organisation determines perceived control on sharing of data					
External Factors					
Willing sharing partners determines perceived control on sharing of data					
Reliable sharing partners determines perceived control on sharing of data					
Compatible purpose of application determines perceived control on sharing of data					
Organisational fit determines perceived control on sharing of data					
AD-SDI awareness creation determines perceived control on sharing of data					
Fora organised by the AD-SDI determines perceived control on sharing of data					

Policy development determines perceived control on sharing of data					
Standards alignment determines perceived control on sharing of data					
Abu Dhabi core data set identification determines perceived control on sharing of data					
Abu Dhabi Spatial Data Directory determines perceived control on sharing of data					

3. Do you think organisation's perceived control on geospatial data sharing is influenced by external and internal factors?

□ Strongly Disagree

□ Disagree

□ Undecided

□ Agree

□ Strongly Agree

Section D: Socio-Demographic Factors

1. Age

□ 20-24 years

□ 25-29 years

□ 30-34 years

□ 35-39 years

□ 40-44 years

□ 45-49 years

□ 50 years and above

2. Gender

□ Male

□ Female

3. Marital Status

□ Now married

□ Widowed

□ Divorced

□ Separated

□ Never married

4. Highest degree or level of school you have completed

□ High school graduate - high school diploma or the equivalent (for example: GED)

□ Associate degree

□ Bachelor's degree

□ Master's degree

□ Professional degree

□ Doctorate degree

5. Position within the Organisation

□ Junior Management Level

□ Middle Management Level

□ Senior Management Level

□ Administrative Position

□ Clerical Position

□ Others____________________

6. Years of Experience in the Organisation

□ 0-5 years

□ 5-10 years

□ 10-15 years

□ 15-20 years

□ 20-25 Years

□ More than 25 years

Thank you for participating!

APPENDIX 2: QUALITATIVE QUESTIONNAIRE

1. Name: ____________________
2. Age: __________________
3. Position held: __________________
4. Years of Experience: _________________

Section A: Role of the AD-SDI in Geospatial Data Sharing of Organisations

1. Reflect on the AD-SDI role in coverage of geospatial data standard.

____

____

2. In what way does this standard benefits the GIS community of Abu Dhabi?

____

____

3. How much pragmatic is AD-SDI in developing the standard to accommodate newer demands?

____

____

Section B: Challenges Related to Data Security

4. AD-SDI in its charter mentions about the significance of security and lists it as one of the standard's benefits. Still, there are lingering issues of information security. Why?

____

____

5. Do you think infrastructure related vulnerabilities (such as single feeder line) affect the security of information shared? Are there any cases as such experienced by you?

____

____

6. Are there any risks related to classification of sensitivity of data? How do you address them?

____

____

Section C: Strategies to Mitigate Security Challenges

7. Highlight some core strategies associated with security risk assessment?

____

____

8. What are the risk management policies you follow to mitigate the existing and predicted challenges? To what extent does that help you in accuracy of prediction?

____

____

9. In what ways do you ensure secure design system by addressing potential challenges?

____

____

10. Do you think collaboration among organisations ensure a faster remedy? How?

____

____

11. State some future scope of development in terms of information security maintenance of geospatial data?

____

____

Any other comments?

____

____

Thank you!

APPENDIX 3: ORGANISATION'S STRATEGIC POSITION

CORRELATION

		Do you think the organisation's strategic position influences its geospatial data sharing ?
Do you think the organisation's strategic position influences its geospatial data sharing?	Pearson Correlation	1
	Sig. (2-tailed)	
	N	200
Loss of Control over Data Sharing		
Sharing leads to loss of control of ownership rights or copyrights	Pearson Correlation	.930**
	Sig. (2-tailed)	.000
	N	200
Sharing leads to regulated access without necessarily owning the resource	Pearson Correlation	.935**
	Sig. (2-tailed)	.000
	N	200
Sharing leads to loss of actual use and control of the resource	Pearson Correlation	.741**
	Sig. (2-tailed)	.000
	N	200
Sharing leads to loss of the ability to rule or regulate possession, allocation and use of the resource and enforcement of legislation	Pearson Correlation	.645**
	Sig. (2-tailed)	.000
	N	200
Behavioural beliefs about knowledge creation		
Sharing leads to creation of explicit to explicit knowledge	Pearson Correlation	.641**
	Sig. (2-tailed)	.000
	N	200
Sharing leads to creation of explicit to tacit knowledge	Pearson Correlation	.894**
	Sig. (2-tailed)	.000
	N	200
Sharing leads to creation of tacit to tacit knowledge	Pearson Correlation	.704**
	Sig. (2-tailed)	.000
	N	200
Sharing leads to creation of tacit to explicit knowledge	Pearson Correlation	.898**
	Sig. (2-tailed)	.000
	N	200
Sharing leads to Inter-organisational relationships in terms of redistribution of relative	Pearson Correlation	.975**
	Sig. (2-tailed)	.000

power and influence in organisational environment	N	200
Sharing leads to integrated development planning	Pearson Correlation	.726**
	Sig. (2-tailed)	.000
	N	200
Sharing leads to distribution of benefits to society at large	Pearson Correlation	.866**
	Sig. (2-tailed)	.000
	N	200
Normative beliefs about GIS community pressure		
Local governmental authorities' GIS users disapprove the organisation's engagement in spatial data sharing	Pearson Correlation	.812**
	Sig. (2-tailed)	.000
	N	200
GIS users of federal government disapprove the organisation's engagement in spatial data sharing	Pearson Correlation	.732**
	Sig. (2-tailed)	.000
	N	200
Municipal GIS users disapprove the organisation's engagement in spatial data sharing	Pearson Correlation	.703**
	Sig. (2-tailed)	.000
	N	200
Para-statal organisations'GIS departments disapprove the organisation's engagement in spatial data sharing	Pearson Correlation	.882**
	Sig. (2-tailed)	.000
	N	200
Private sector GIS users disapprove the organisation's engagement in spatial data sharing	Pearson Correlation	.801**
	Sig. (2-tailed)	.000
	N	200
NGO GIS users disapprove the organisation's engagement in spatial data sharing	Pearson Correlation	.918**
	Sig. (2-tailed)	.000
	N	200
Academic research institutions' GIS users disapprove the organisation's engagement in spatial data sharing	Pearson Correlation	.882**
	Sig. (2-tailed)	.000
	N	200
Normative beliefs about Market pressure		
	Pearson Correlation	.648**

Commercial spatial data brokers disapprove organisation’s engagement in spatial data sharing	Sig. (2-tailed)	.000
	N	200
Public spatial data providers disapprove organisation’s engagement in spatial data sharing	Pearson Correlation	.907**
	Sig. (2-tailed)	.000
	N	200
Private spatial data providers disapprove organisation’s engagement in spatial data sharing	Pearson Correlation	.885**
	Sig. (2-tailed)	.000
	N	200
GIS suppliers disapprove organisation’s engagement in spatial data sharing	Pearson Correlation	.591**
	Sig. (2-tailed)	.000
	N	200
Normative beliefs about Institutional pressure		
AD-SDI disapprove organisation’s engagement in spatial data sharing	Pearson Correlation	.739**
	Sig. (2-tailed)	.000
	N	200
Spatial data agreements disapprove organisation’s engagement in spatial data sharing	Pearson Correlation	.731**
	Sig. (2-tailed)	.000
	N	200
Normative beliefs about organisational pressure		
Politicians disapprove organisation’s engagement in spatial data sharing	Pearson Correlation	.713**
	Sig. (2-tailed)	.000
	N	200
Other departments within same organisation disapprove organisation’s engagement in spatial data sharing	Pearson Correlation	.756**
	Sig. (2-tailed)	.000
	N	200
Management of the organisation disapprove organisation’s engagement in spatial data sharing	Pearson Correlation	.439**
	Sig. (2-tailed)	.000
	N	200
Individual champions for sharing disapprove organisation’s engagement in spatial data sharing	Pearson Correlation	.699**
	Sig. (2-tailed)	.000
	N	200
Mandate (organisational goals/mission) disapprove organisation’s engagement in spatial data sharing	Pearson Correlation	.761**
	Sig. (2-tailed)	.000
	N	200
Perceived moral norms		

Sharing is perceived as an obligation for the sake of integrated development planning	Pearson Correlation	.934**
	Sig. (2-tailed)	.000
	N	200
Sharing is perceived as an obligation for the sake of society at large	Pearson Correlation	.841**
	Sig. (2-tailed)	.000
	N	200

APPENDIX 4: ORGANISATION'S STRATEGIC POSITION

COEFFICIENTS

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.290	.051		-5.699	.000
	Loss of Control over Data Sharing					
	Sharing leads to loss of control of ownership rights or copyrights	.106	.025	.100	4.252	.000
	Sharing leads to regulated access without necessarily owning the resource	.062	.026	.060	2.355	.020
	Sharing leads to loss of actual use and control of the resource	-.002	.013	-.003	-.192	.848
	Sharing leads to loss of the ability to rule or regulate possession, allocation and use of the resource and enforcement of legislation	.039	.009	.047	4.253	.000
	Behavioural beliefs about knowledge creation					
	Sharing leads to creation of explicit to explicit knowledge	-.038	.012	-.046	-3.194	.002
	Sharing leads to creation of explicit to tacit knowledge	.078	.017	.085	4.621	.000
	Sharing leads to creation of tacit to tacit knowledge	.009	.011	.010	.786	.433
	Sharing leads to creation of tacit to explicit knowledge	.050	.019	.053	2.613	.010

	Sharing leads to Inter-organisational relationships in terms of redistribution of relative power and influence in organisational environment	.233	.041	.228	5.625	.000
	Sharing leads to integrated development planning	.023	.014	.025	1.644	.102
	Sharing leads to distribution of benefits to society at large	.038	.017	.041	2.184	.030
	Normative beliefs about GIS community pressure					
	Local governmental authorities' GIS users disapprove the organisation's engagement in spatial data sharing	-.005	.026	-.005	-.192	.848
	GIS users of federal government disapprove the organisation's engagement in spatial data sharing	-.012	.013	-.013	-.924	.357
	Municipal GIS users disapprove the organisation's engagement in spatial data sharing	.003	.014	.004	.238	.812
	Parastatal organisations' GIS departments disapprove the organisation's engagement in spatial data sharing	-.002	.030	-.002	-.061	.952
	Private sector GIS users disapprove the organisation's engagement in spatial data sharing	.029	.016	.030	1.831	.069
	NGO GIS users disapprove the organisation's engagement in spatial data sharing	.115	.035	.124	3.313	.001

	Academic research institutions’ GIS users disapprove the organisation’s engagement in spatial data sharing	.020	.032	.020	.618	.537
	Normative beliefs about Market pressure					
	Commercial spatial data brokers disapprove organisation’s engagement in spatial data sharing	.010	.012	.012	.883	.379
	Public spatial data providers disapprove organisation’s engagement in spatial data sharing	.064	.017	.070	3.705	.000
	Private spatial data providers disapprove organisation’s engagement in spatial data sharing	.044	.020	.038	2.150	.033
	GIS suppliers disapprove organisation’s engagement in spatial data sharing	.019	.012	.021	1.610	.100
	Normative beliefs about Institutional pressure					
	AD-SDI disapprove organisation’s engagement in spatial data sharing	.029	.012	.035	2.359	.019
	Spatial data agreements disapprove organisation’s engagement in spatial data sharing	.009	.012	.011	.739	.461
	Politicians disapprove organisation’s engagement in spatial data sharing	-.010	.015	-.011	-.658	.511
	Normative beliefs about organisational pressure					
	Other departments within same organisation disapprove organisation’s engagement in spatial data sharing	.037	.017	.041	2.191	.030

	Management of the organisation disapprove organisation’s engagement in spatial data sharing	.017	.009	.018	1.895	.060
	Individual champions for sharing disapprove organisation’s engagement in spatial data sharing	.026	.010	.029	2.485	.014
	Mandate (organisational goals/mission) disapprove organisation’s engagement in spatial data sharing	.003	.014	.004	.231	.817
	Perceived moral norms					
	Sharing is perceived as an obligation for the sake of integrated development planning	.046	.024	.046	1.861	.064
	Sharing is perceived as an obligation for the sake of society at large	.050	.014	.053	3.561	.000

a. Dependent Variable: Do you think the organisation's strategic position influences its geospatial data sharing ?

APPENDIX 5: ORGANISATION'S PERCEIVED CONTROL CORRELATION

		Do you think organisation's perceived control on geospatial data sharing is influenced by external and internal factors?
Do you think organisation's perceived control on geospatial data sharing is influenced by external and internal factors?	Pearson Correlation	1
	Sig. (2-tailed)	
	N	200
Internal Factors		
Assessing of quality of spatial data determines perceived control on sharing of data	Pearson Correlation	.927**
	Sig. (2-tailed)	.000
	N	200
Handling different formats of spatial data determines perceived control on sharing of data	Pearson Correlation	.716**
	Sig. (2-tailed)	.000
	N	200
Mastering different standards determines perceived control on sharing of data	Pearson Correlation	.681**
	Sig. (2-tailed)	.000
	N	200
Selection of spatial data for exchange determines perceived control on sharing of data	Pearson Correlation	.782**
	Sig. (2-tailed)	.000
	N	200
Integration of different spatial data sets determines perceived control on sharing of data	Pearson Correlation	.754**
	Sig. (2-tailed)	.000
	N	200
Interpretation of metadata to establish its adequacy determines perceived control on sharing of data	Pearson Correlation	.807**
	Sig. (2-tailed)	.000
	N	200
Usage of metadata interfaces /databases determine perceived control on sharing of data	Pearson Correlation	.914**
	Sig. (2-tailed)	.000
	N	200
Capturing of metadata determines perceived control on sharing of data	Pearson Correlation	.747**
	Sig. (2-tailed)	.000
	N	200
Application of metadata standards determines	Pearson Correlation	.752**
	Sig. (2-tailed)	.000

perceived control on sharing of data	N	200
Maintenance/updating of metadata of metadata standard determines perceived control on sharing of data	Pearson Correlation	.910**
	Sig. (2-tailed)	.000
	N	200
Database administration determines perceived control on sharing of data	Pearson Correlation	.863**
	Sig. (2-tailed)	.000
	N	200
Using the internet to locate spatial data source determines perceived control on sharing of data	Pearson Correlation	.876**
	Sig. (2-tailed)	.000
	N	200
Using the internet to distribute spatial data determines perceived control on sharing of data	Pearson Correlation	.629**
	Sig. (2-tailed)	.000
	N	200
Transfer of spatial data to/from different media determines perceived control on sharing of data	Pearson Correlation	.628**
	Sig. (2-tailed)	.000
	N	200
Establishment/fostering of contacts determines perceived control on sharing of data	Pearson Correlation	.651**
	Sig. (2-tailed)	.000
	N	200
Identification of meeting opportunities determines perceived control on sharing of data	Pearson Correlation	.334**
	Sig. (2-tailed)	.000
	N	200
Collaboration with other determines perceived control on sharing of data	Pearson Correlation	.596**
	Sig. (2-tailed)	.000
	N	200
Collaboration with other determines perceived control on sharing of data	Pearson Correlation	.657**
	Sig. (2-tailed)	.000
	N	200
Pricing of spatial data determines perceived control on sharing of data	Pearson Correlation	.624**
	Sig. (2-tailed)	.000
	N	200
Data ownership agreement determines perceived control on sharing of data	Pearson Correlation	.731**
	Sig. (2-tailed)	.000
	N	200
Liability agreements determines perceived control on sharing of data	Pearson Correlation	.689**
	Sig. (2-tailed)	.000
	N	200
Bad experiences with spatial data sharing with other organisations	Pearson Correlation	.636**
	Sig. (2-tailed)	.000

determines perceived control on sharing of data	N	200
Sufficient Staff determines perceived control on sharing of data	Pearson Correlation	.557**
	Sig. (2-tailed)	.000
	N	200
Availability of funding determines perceived control on sharing of data	Pearson Correlation	.023
	Sig. (2-tailed)	.749
	N	200
Organisational guidelines determine perceived control on sharing of data	Pearson Correlation	.876**
	Sig. (2-tailed)	.000
	N	200
Control beliefs about dependence on spatial data		
Importance of spatial data to own organisation determines perceived control on sharing of data	Pearson Correlation	.400**
	Sig. (2-tailed)	.000
	N	200
Copyright determine perceived control on sharing of data	Pearson Correlation	.652**
	Sig. (2-tailed)	.000
	N	200
Regulated access determine perceived control on sharing of data	Pearson Correlation	.655**
	Sig. (2-tailed)	.000
	N	200
Availability of alternative sources determine perceived control on sharing of data	Pearson Correlation	.672**
	Sig. (2-tailed)	.000
	N	200
Stability of alternative sources determine perceived control on sharing of data	Pearson Correlation	.786**
	Sig. (2-tailed)	.000
	N	200
Spatial data self-sufficiency of the organisation determines perceived control on sharing of data	Pearson Correlation	.631**
	Sig. (2-tailed)	.000
	N	200
External Factors		
Willing sharing partners determine perceived control on sharing of data	Pearson Correlation	.838**
	Sig. (2-tailed)	.000
	N	200
Reliable sharing partners determine perceived control on sharing of data	Pearson Correlation	.882**
	Sig. (2-tailed)	.000
	N	200
Compatible purpose of application determines perceived control on sharing of data	Pearson Correlation	.709**
	Sig. (2-tailed)	.000
	N	200

Organisational fit determines perceived control on sharing of data	Pearson Correlation	.852**
	Sig. (2-tailed)	.000
	N	200
AD-SDI awareness creation determines perceived control on sharing of data	Pearson Correlation	.703**
	Sig. (2-tailed)	.000
	N	200
Fora organised by the ADSIC determines perceived control on sharing of data	Pearson Correlation	.758**
	Sig. (2-tailed)	.000
	N	200
Policy development determines perceived control on sharing of data	Pearson Correlation	.876**
	Sig. (2-tailed)	.000
	N	200
Standards alignment determines perceived control on sharing of data	Pearson Correlation	.702**
	Sig. (2-tailed)	.000
	N	200
Abu Dhabi core data set identification determines perceived control on sharing of data	Pearson Correlation	.957**
	Sig. (2-tailed)	.000
	N	200
Abu Dhabi Spatial Data Directory determines perceived control on sharing of data	Pearson Correlation	.618**
	Sig. (2-tailed)	.000
	N	200

APPENDIX 6: ORGANISATION'S PERCEIVED CONTROL COEFFICIENTS

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.045	.057		-.789	.431
	Internal Factors					
	Assessing of quality of spatial data determines perceived control on sharing of data	.106	.024	.108	4.445	.000
	Handling different formats of spatial data determines perceived control on sharing of data	-.120	.060	-.124	-2.013	.046
	Mastering different standards determines perceived control on sharing of data	-.051	.014	-.057	-3.520	.001
	Selection of spatial data for exchange determines perceived control on sharing of data	-.486	.055	-.505	-8.916	.000
	Integration of different spatial data sets determines perceived control on sharing of data	-.005	.016	-.005	-.306	.760
	Interpretation of metadata to establish its adequacy determines perceived control on sharing of data	.488	.057	.516	8.480	.000
	Usage of metadata interfaces/databases determines perceived control on sharing of data	-.135	.125	-.132	-1.077	.283
	Capturing of metadata determines perceived control on sharing of data	.006	.011	.007	.521	.603

	Application of metadata standards determines perceived control on sharing of data	-.024	.066	-.027	-.373	.710
	Maintenance/updating of metadata of metadata standard determines perceived control on sharing of data	.253	.122	.249	2.071	.040
	Database administration determines perceived control on sharing of data	.023	.056	.024	.407	.685
	Using the internet to locate spatial data source determines perceived control on sharing of data	.134	.057	.145	2.336	.021
	Using the internet to distribute spatial data determines perceived control on sharing of data	.001	.012	.001	.093	.926
	Transfer of spatial data to/from different media determines perceived control on sharing of data	-.012	.014	-.013	-.842	.401
	Establishment/fostering of contacts determines perceived control on sharing of data	.011	.016	.013	.732	.465
	Identification of meeting opportunities determines perceived control on sharing of data	.007	.009	.008	.810	.419
	Collaboration with other determines perceived control on sharing of data	.175	.032	.196	5.418	.000
	Collaboration with other determines perceived control on sharing of data	-.004	.013	-.004	-.303	.763
	Pricing of spatial data determines perceived control on sharing of data	-.369	.054	-.412	-6.800	.000
	Data ownership agreement determines perceived control on sharing of data	.064	.037	.068	1.759	.081

	Liability agreements determines perceived control on sharing of data	-.068	.034	-.072	-2.013	.046
	Bad experiences with spatial data sharing with other organisations determines perceived control on sharing of data	.383	.054	.416	7.096	.000
	Sufficient Staff determines perceived control on sharing of data	-.168	.031	-.187	-5.360	.000
	Availability of funding determines perceived control on sharing of data	-.013	.007	-.017	-2.030	.044
	Organisational guidelines determine perceived control on sharing of data	.001	.065	.001	.019	.985
	Control beliefs about dependence on spatial data					
	Importance of spatial data to own organisation determines perceived control on sharing of data	-.001	.008	-.001	-.085	.932
	Copyright determines perceived control on sharing of data	-.362	.082	-.415	-4.444	.000
	Regulated access determines perceived control on sharing of data	.298	.060	.341	4.920	.000
	Availability of alternative sources determines perceived control on sharing of data	.127	.054	.144	2.332	.021
	Stability of alternative sources determines perceived control on sharing of data	.056	.019	.061	2.952	.004
	Spatial data self-sufficiency of the organisation determines perceived control on sharing of data	.014	.011	.015	1.186	.237

	External Factors					
	Willing sharing partners determines perceived control on sharing of data	.014	.020	.015	.677	.500
	Reliable sharing partners determines perceived control on sharing of data	.029	.082	.029	.350	.726
	Compatible purpose of application determines perceived control on sharing of data	.074	.013	.080	5.784	.000
	Organisational fit determines perceived control on sharing of data	.099	.020	.105	4.986	.000
	AD-SDI awareness creation determines perceived control on sharing of data	-.006	.023	-.006	-.242	.809
	Fora organised by the AD-SDI determines perceived control on sharing of data	-.090	.073	-.099	-1.238	.218
	Policy development determines perceived control on sharing of data	.054	.017	.058	3.140	.002
	Standards alignment determines perceived control on sharing of data	.041	.059	.043	.690	.491
	Abu Dhabi core data set identification determines perceived control on sharing of data	.465	.032	.465	14.575	.000
	Abu Dhabi Spatial Data Directory determines perceived control on sharing of data	.004	.012	.004	.291	.772

a. Dependent Variable: Do you think organisation's perceived control on geospatial data sharing is influenced by external and internal factors?