The use of TRAO to Manage Evolution Risks in E-Government

By

Onyekachi Chinemerem Onwudike

A Doctoral Thesis

Submitted in partial fulfilment of the requirements for the award of

Doctor of Philosophy of Loughborough University

2018

Dedication

To my loving parents, Ogbonnaya Onwudike and Nwakaku Onwudike whose love, unselfish support and examples over many years have given me the strength to complete this work.

To my husband Chris and my son Daniel, by far the most invaluable assets I acquired during the course of my PhD.

Abstract

The need to develop and provide more efficient ways of providing Electronic Government Services to key stakeholders in government has brought about varying degrees of evolution in government. This evolution is seen in different ways like the merging of government departments, the merging of assets or its components with legacy assets etc. This has involved the incorporation of several practices that are geared towards the elimination of processes that are repetitive and manual while attempting to progressively encourage the interaction that exists between the different stakeholders. However, some of these practices have further complicated processes in government thus creating avenues for vulnerabilities which if exploited expose government and government assets to risks and threats.

Focusing on ways to manage the issues accompanied with evolution can better prepare governments for manging the associated vulnerabilities, risks and threats. The basis of a conceptual framework is provided to establish the relationships that exist between the E-Government, asset and security domains. Thus, this thesis presents a design research project used in the management of evolution-related risks. The first part of the project focusses on the development of a generic ontology known as TRAO and a scenario ontology TRAOSc made up of different hypothetical scenarios. The resulting efficiency of the development of these ontologies have facilitated the development of an intelligent tool TRAOSearch that supports high-level semantically enriched queries.

Results from the use of a case study prove that there are existing evolution-related issues which governments may not be fully prepared for. Furthermore, an ontological approach in the management of evolution-related risks showed that government stakeholders were interested in the use of intelligent processes that could improve government effectiveness while analysing the risks associated with doing this. Of more importance to this research was the ability to make inferences from the ontology on existing complex relationships that exist in the form of dependencies and interdependencies between Stakeholders and Assets.

Thus, this thesis presents contributions in the aspect of advancing stakeholders understanding on the types of relationships that exist in government and the effect these relationships may have on service provisioning. Another novel contribution can be seen in the correction of the ambiguity associated with the terms Service, IT Service and E-Government. Furthermore, the feedback obtained from the use of an ontology-based tool

during the evaluation phase of the project provides insights on whether governments must always be at par with technological evolution.

Keywords: E-Government, E-Government Services, Stakeholders, Asset, Risk, Vulnerability, Threat, Ontology, Evolution.

Acknowledgements

This thesis is the peak of my journey of a PhD which can be likened to climbing a flight of stairs accompanied by hard work, hardship, frustration, efforts, tears, commitment, trust, encouragement and sheer belief. The experience of fulfilment and gratitude that I feel today is borne out of the passion to move me to a whole new level and although only my name now appears on the cover of this thesis, I cannot but acknowledge the contributions of the people and organisations that have helped me achieve this great feat.

I am extremely indebted to my Supervisors, Dr Russell Lock and Dr Iain Phillips for all the invaluable guidance during the course of this research and for constantly pointing me to the right path. I am extremely thankful to Russell whose support enabled me to successfully overcome the many difficulties during this research. In his words 'go forth'. Thank you for your guidance Russell. Thank you for spurring me on to perfection, thank you for your constant involvement in my research, thank you for your sheer belief in me and thank you for always inspiring me to do more. You exposed me to an entirely different aspect of life and it's amazing how far one can go when someone believes in you. In the words of a writer "Good people are like candles; they burn themselves up to give others light". It will be foolishness to deny your goodness to me and for that I remain indebted to you.

Without the right materials in place, I would not have been able to successfully complete this research. For this reason, I am grateful to the staff and management of Loughborough University for putting in place adequate resources and infrastructure that enabled me successfully carry out this research.

My sincere thanks go to the members of the Government Digital Service and the Nationwide Building Society who were involved in discussing, supporting and evaluating my research.

I am extremely grateful to my parents Prof and Pharm(Mrs) Onwudike who completely funded my PhD and have constantly defied all odds in training the girl-child. I salute you for your courage, selfless sacrifice and love and I am eternally indebted to you for the seeds you have sown in my life. Thank you for praying for me, cheering me on and for believing in me even when my belief in myself began to dwindle.

I am thankful to my sisters Oluchi, Chinyere, Nnenna and Chidinma; my brothers in law Austin, Nd, Ifeanyi and Pascal whose constant love, encouragement and assistance contributed to the successful completion of my thesis.

I am thankful to my in-laws for their constant support and encouragement. Some special words of gratitude go to my friends and to the members of Fuyin who were such great support especially Denise who always took my son Daniel, so I could have some time to study.

I am thankful for my Uncle Enyi Onuoha who was always available for me during my research and constantly paid me visits to be sure I was keeping well.

To my mentor of blessed memory Dr (Mrs) Martha Cheo, years ago we discussed what your PhD journey involved. Thoughts of your strength and resilience in your quest for knowledge sustained me. I wish you were here for me to say, “I did it”.

To my mother in-law of blessed memory, you reminded me each time that you were praying for me. Thank you for praying for me and with me. I have the tangible results of your prayers in my hand now.

Last but not the least, I would like to express my sincere gratitude to my husband Chris and my son Daniel. Without question, you both are the most invaluable assets I have acquired in my quest for this PhD. I am thankful for your support, understanding and love throughout this PhD. You’ve both shared in my joys and pain and I can never thank you enough.

Dear God, thank you. Thank you for constantly reminding me that your timing for me is perfect. You are never early or late. You are always right on time and you make everything beautiful at the right time. This journey has taken a lot of patience and a lot of faith, but it’s been worth the wait.

Table of Content

Table of Figures

List of Tables

PART I: INTRODUCTION AND SCOPE OF RESEARCH

Chapter 1: Introduction

There is often the assumption that to make a success of government, government needs to go digital (Andrews et al. 2016; Corydon et al. 2016) because it is believed that making government digital has a way of transforming government services and systems (Hall, 2016). As efforts are ongoing to provide digital/electronic services in ways that eliminate processes that are manual and repetitive whilst providing services that reflect present-day modern society, it is equally important to analyse the risks that may emanate from digitalising government (Public Governance and Territorial Development Directorate 2014; National Audit Office 2017a).

There is the need to develop more efficient ways of providing Electronic Government Services (from this point referred to as EGov Services) which has increased the use of technology in the organisations within government. There is also growing recognition of the need for systems to evolve to meet new challenges (Eggers and Macmillan, 2015; Haan 2015; Margetts 2017). Approaches involving the use of technology as a tool are being adopted by governments around the world to provide users (citizens, businesses, government organisations) with services that are more accessible (Walsham 2013; Tohidi 2011; Chan et al. 2010). These evolving practices involve the increasing and continuous evolution of components[1], systems, platforms[2] and infrastructures[3] on which the EGov Services run. Although these evolutions are geared towards providing more efficient services, they come with associated problems and complexities.

This study investigates how evolution in government with the use of modern and emerging practices can be accompanied by risks[4] and why governments need to pay attention to the assets[5] that are used in promoting service delivery. Furthermore, this thesis contributes to managing evolution-related risks by presenting the results of a design research project which involves the development of a domain ontology for linking IT Assets, IT Services, EGov Services, Stakeholders and Risks which are later instantiated into a software tool. The prototype tool is developed based on scenarios formulated in the development of the ontology and it is evaluated against a government department to demonstrate its

[1] a component is part of something more complex. A system can be part of a larger system
[2] Platforms exist to solve problems common to all or many government departments. They are interconnected components of a larger system (Singleton 2015).
[3] For this research, this refers to networks or platforms
[4] *"the effect of uncertainty on objectives"* (ISO 31000 2009)
[5] " *an item, thing or entity that has potential or actual value to an organisation"* (ISO 55000 2014)

significance. Thus, providing insights on the effectiveness of the ontological approach in managing evolution-related risks.

1.1 Research Motivation

The concept of Electronic Government is well established. The term Electronic Government (henceforth referred to as E-Government) is often synonymous in practice and literature with the implementation of EGov Services. For this research, these terms are defined to be separate but interrelated concepts.

Most of the examples used in this research have been drawn from the UK Government considering that it is one of the most digitally advanced governments in the world and is known to be one of the world leaders in the provision of digital public services (Cabinet Office United Kingdom 2014)[6]. Despite the reported potential of technology in transforming the operations of a government, there are still areas that attention must be paid to. This section presents some of these problems with examples of attempts made by governments to address these problems. Additional examples are discussed in section 2.4. Although this is not an exhaustive set of the problems, this sets the background for the research motivation.

- the need to integrate standalone & evolving services to provide more complex services that are integrated as well as effective and efficient (Asa'd M. As'ad et al. 2017; Halligan & Moore 2004; Sanati & Lu 2007; Sarikas & Weerakkody 2007; House of Commons 2013; UK Government Cabinet Office 2013). A typical example is seen in the attempts made at integration in the National Health Service (NHS) where a person's care may be provided by several health and social care professionals across different providers of the service[7] (Suter et al. 2009; UK Government Cabinet Office 2013; Welsh Government news 2015);
- the need to integrate the systems and infrastructure on which these services run which involves integrating the information systems on which these services run (NHS

[6] The countries that have advanced governments came together to form the D5 charter while committing to working towards the principles of digital development. The founding members are United Kingdom, South Korea, Estonia, Israel and New Zealand (UK Government Cabinet Office 2014).

[7] http://www.adsscymru.org.uk/media-resources-list/6-7m-investment-in-new-it-system-to-integrate-nhs-and-social-services-in-wales/
https://www.kingsfund.org.uk/projects/verdict/how-far-has-government-gone-towards-integrating-care
Reasons for integrating the systems of the National Health Service (NHS) in the United Kingdom (NHS Monitor 2015; Frontier Economics Ltd 2012): i. To eliminate duplication and gaps in service delivery, ii. To avoid people getting lost in the system, iii. To avoid delays, iv. To avoid duplication and repetition

Alliance 2008) so that the infrastructure gap[8] that exists between old and new infrastructure can be eliminated and interoperability[9] amongst these systems or infrastructures encouraged (OECD 2003; Cabinet Office United Kingdom 2011);

- the need to eliminate silos between service providing organisations by building bridges across them and encouraging communication between them (Pattison 2006);
- the lack of reuse[10] and adaptation of systems which are available 'off the shelf' by Service Providers (Departments, agencies, public bodies, organisations) leading to waste (Airey 2015; Adewunmi 2015; Lampathaki et al. 2010; Cabinet Office United Kingdom 2011). A typical example of a case where duplication has proven to be wasteful can be seen in the case where the Ministry of Justice in the UK had to write off the sum of £56 million after the discovery that the project was over budget, late and duplicated by another government department (Syal 2014);

  Some examples of attempts at reusing systems and infrastructure within the Department for Work and Pensions (DWP) and the HM Revenue and Customs (HMRC) in the UK include the National Insurance Recording System, The Customer Information System & Payment Infrastructure;
- the need to eliminate the use of dysfunctional systems[11] and organisations in government (Service Manual UK 2016). Examples of dysfunctional systems are seen in the Justice system in the UK, local authority systems in the UK (Topping 2015);
- the need for governments to handle smaller ICT projects as opposed to large projects so that risks of failures associated with handling such projects may be reduced. With large ICT projects, there is the tendency for them to become gigantic, complex and consequently difficult to manage (Holgeid & Thompson 2013). According to a report produced by PASC, 6 underlying reasons for failure were identified[12] (PASC 2011);

[8] Infrastructure gap *"is frequently used to indicate the current need for investments in infrastructure"* (Silva 2017)
[9] "*The ability for subsystems to exchange data at the technical level using shared protocols and networks. Sometimes embraces data integrability" -(*ISEB 2010).
[10] *"re-use means any operation by which products or components that are not waste are used again for the same purpose for which they were conceived"* (Defra 2014)
[11] Dysfunctional systems may be seen as systems whose costs act as a barrier to the achievement of a service (Telegraph View 2015) or systems where their allotted costs are invested in services where they are not needed (Hickie 2017). They can also be referred to systems that do not work the way they should.
https://www.theguardian.com/society/2015/jun/03/no-recourse-to-public-funds-children-poverty-uk-government
http://www.telegraph.co.uk/news/uknews/law-and-order/11694744/Our-legal-system-is-dysfunctional-and-must-be-reformed.html
[12] Reasons for failure:

i. Inadequate information, resulting in the Government being unable to manage its IT needs successfully
ii. Over-reliance on a small number of large suppliers and the virtual exclusion of small and medium sized (SME) IT contractors, which tend to be less risk adverse and more innovative;
iii. Inability to integrate IT into the wider policy and business change programmes;

- the need to resolve the challenges to data integration where there is need to synchronize heterogenous, variable and big data (Lexis Nexis 2010; U.S. Department of Transportation & Administration 2010);

The design of an E-Government Service dictates the need for systems. Thus, the development of large scale systems should be accompanied with support for evolution (Friedman 2016; Han & Chen 2002; Sommerville 2004; Pittas et al. 2001). Systems that are said to be sustainable may be subject to ongoing change and these changes can take place for a variety of reasons (London 1996; Mockus & Votta 2000; Hough 2014; Harries et al. 2015). Some of these changes as identified in literature include:

- redundancy and decommissioning of systems (NWSI 80-202 2014);
- replacement of system components (Robey et al. 2002);
- evolution of a system occurring at multiple levels and within multiple levels of the system (Lock 2012);
- changes to a system because of dependent systems (Lock & Sommerville 2010);
- expansion of the system to incorporate new services (Raleigh, 2015)
- the need to acquire systems that are more resilient (IBM News Room 2016);
- inclusion of a new function (Krell et al. 2008);
- a shift of the business system toward true sustainability (Waddock 2013);
- lack of support for current business needs (Svensson 2016);
- software withdrawal and support discontinuance (IBM United States 2014; Emis Health 2014);
- issues related to system resilience and adaptiveness (Chapin et al. 2010);
- changes in user needs and requirements (Sommerville 2000; Kramer & Magee 1985);
- evolution and changes to standards (Lock 2011) amongst others.

During system evolution, the rationale behind the original development of a system may be superseded because of changes in circumstances which may not have been foreseen from the initial development of the system.

iv. A tendency to commission large, complex projects which struggle to adapt to changing circumstances;
v. over-specification of security requirements;
vi. The lack of sufficient leadership and skills to manage IT within the Civil Service, and the absence of an "intelligent customer" function in Departments

As change takes place in government systems, one of the ways to combat the challenges that may be encountered with these changing systems is to engage evolving practices such as encouraging reuse across these systems. But reuse also comes with its associated challenges. Reuse of systems, components, platforms, infrastructures allow for dependencies and interdependencies across systems. Although attempts have also been made by governments to provide integrated services[13] which may be made possible by reusing solutions, this has its own disadvantages.

Understanding that a system may be made up of several components which independently may be systems is important[14]. Each component may either be an independent system or a component of another system or both[15]. Simply put, a system can be a component and a component can also be a system. Also, the ability of a system to function may depend on the availability of other systems or components. Therefore, the issue of dependency must be considered. There may be cases where a System (S_1) depends on System ($S_{3)}$ for an EGov Service (ES_1) to run; this dependency doesn't necessarily mean that (S_1) depends on the entirety of ($S_{3)}$ to function. It simply means that a part of ($S_{3)}$ which may be a component is required for the delivery of EGov Service (ES_1). For this explanation, this thesis has made use of the word *system* only. From the explanation on systems being composed of components/systems, there are cases where to accommodate the evolutions across these systems, there are resultant failures across components, systems and infrastructures which in turn may lead to cascading failures[16] and service disruptions. However, it should be noted that this explanation applies to assets, a concept which is explained in detail in chapter 3. The explanation is a guide to help the reader understand how a failure of one component may result in several other failures. These issues occur because of the complexity, the increase in the number of components, interconnectedness, dependent and interdependent nature of these systems (Johansson 2010; Blackwell 2008). This thesis is focussed on capturing and explicating these identified evolution challenges using a novel approach. The issue of managing evolving complexities with evolving systems or with existent legacy systems, the kinds of risks that can emanate from reuse within and across systems and even

[13] "*the result of bringing together – and fitting together – government services so that citizens can access them in a single seamless experience based on their wants and needs"* (Kernaghan 2012)
[14] System 1 (S_1) may consist of 15 different components (C_1, C_2, C_3……., C_{15});
[15] C_2 which is one of the components of S_1 is also an independent system that may be composed of other components (C_6, C_7, $C_{8,}$ $C_{9,}$ $C_{10,}$ $C_{17.}$)
[16] Where the failure of one system is the cause of the failure of other systems connected to it which may eventually lead to the partial or complete unavailability of the second system.

across and within Service Providers ((hereafter referred to as SPs) are areas this research attempts to address.

1.2 Research Aims and Research Questions

Following on from the motivations for this research and the problems this research seeks to address the underlying assumptions are that:

i. technology plays a vital role in the way E-Government evolves;
ii. this evolution is focussed majorly on improving the way government services are delivered;
iii. this evolution affects assets (components/systems/infrastructures/platforms) in terms of risks since these assets may be subject to evolution too;
iv. these risks have the potential to negatively influence a service.

This research puts up the argument that to meet the demands of evolving services in E-Government, the following must be understood:

i. the departments that are responsible for individual services;
ii. the departments that own the assets and are responsible for their management;
iii. the relationships that departments have with other departments;
iv. the impacts the relationship between departments have on a service;
v. the relationships that exist between IT services and EGov Services;
vi. the risks, threats and vulnerabilities the assets responsible for running and delivering these services are faced with if a service evolves;

The aim of the research is to analyse what happens as assets (component, systems, platforms, infrastructures) continuously evolve in terms of risks and vulnerabilities using an ontology. The results of this are presented in Chapter 7.

Identifying vulnerable assets or assets that may pose a risk or threat can help in mitigating vulnerabilities that can be classified as high risk. However, to identify what assets are responsible for delivery of services, what assets may be compromised, or the impact evolution may have on a service, it is important to understand what organisations own them or are responsible for their management. Since identifying individual assets may involve difficult and complicated processes, this study develops the following overarching research question:

How can governments identify assets or services that are susceptible to risks if these assets or services in governments must evolve, and what impacts does this evolution have on services?

This question is broken down into different parts to understand the aim of the thesis.

Part one of the question - *How can governments identify assets or services* - the focus of this question is on identifying E-Government assets and services. The Research Questions (RQ) linked to this question are presented in RQ1.

RQ1 Who owns a service and who is responsible for its management?

a) *What assets does a service require to run on?*
b) *Does a service require more than one asset to be in place?*
c) *How can it be established which department owns a particular asset for a service to be delivered?*

Part two of the question - How can governments identify assets or services *that are susceptible to risks* – the focus of this part of the question is on assets and services that are prone to risk especially when the relationships an asset has with other assets has been established and how complex these relationships may be. It must be established if an asset is vulnerable to a risk, and what kind of risks an asset may be exposed to.

To establish this, this study needs to answer questions such as shown in RQ2 and RQ3:

RQ2 What are the risks associated with vulnerable assets?

a) *How vulnerable are assets that are dependent on other assets?*
b) *What are the risks associated with dependencies of single/complex systems, components or infrastructures?*
c) *How can the risks associated with single/complex systems be analysed?*
d) *What kind of risks occur if a service or system is decommissioned?*
e) *Can levels of risks or threats introduced through dependencies and interdependences that exist between vulnerable assets be measured?*
f) *Can potential risks be identified if vulnerable assets are reused?*

RQ3 How can the complexity of multiple dependent assets be managed?

a) *Do dependencies introduce more risks and vulnerabilities to the systems in government?*
b) *Does the composition of single/complex systems, components and infrastructure reveal dependencies and interdependencies that exist between systems in a government?*
c) *Can single/complex dependent systems be identified to see if they have adequate support for their survival if they are detached from other systems or networks?*
d) *Can the effects of resource dependence be measured in terms of costs?*

Part 3 of the question - How can governments identify assets or services that are susceptible to risks *if these assets or services in governments must evolve* - the focus of this part of the question is on the evolution risks that may occur as changes are incorporated which may be accompanied by the evolution of assets as well. This is discussed in section 1.1.

This question sets some delimitation on the scope of the study. It is important to identify all assets and services that are prone to risk during the lifetime of an asset or a service. However, this question limits the scope of this thesis to only the evolutionary stages of assets and services and focusses on only evolutionary risks. To establish this, the study is interested in answering the questions in RQ4.

RQ4 How prepared are governments in the management of evolution-related risks?

a) *What are the types of evolution-related risks that occur as services evolve?*
b) *What kind of risks can reuse of assets introduce?*
c) *What impact does an evolving service or asset have on other services or assets?*
d) *As services evolve, can other services or departments be used as backups in case a failure occurs?*
e) *As services evolve, is it possible to identify what assets can be used as backups if a service must be decommissioned?*

Part 4 of the question - How can governments identify assets or services that are susceptible to risks if these assets or services in governments must evolve *and what impacts does this evolution have on services?* This part of the question is focussed on the impacts of evolution risks and what effect it has on the delivery of a service. Addressing these different questions are important in justifying the motivation for this research and although different methods and models have been used to tackle these challenges from different bodies of research and

schools of thought; this study is interested in identifying these complexities as they relate to Government with the use of an ontology.

These questions RQ5 and RQ6 are answered based on the development of an ontology known as the **Threat Risk and Asset Ontology (TRAO)**:

RQ5 Can a model from the ontology be developed from the results of the research and applied to government systems?

a) *Can patterns of resource or system dependence be obtained from the modelling?*
b) *Can the queries generated from the ontology be applied to real world data?*

RQ6 Does the ontology demonstrate how much change a system can accommodate?

a) *Does the ontology model services or departments that can be used as backups if a failure occurs?*
b) *Does the ontology model services or departments that can be used as backups if a service or system on which a service runs are decommissioned?*
c) *Does the ontology show the risks associated with reuse of service components and infrastructures*?
d) *Can the ontology be used to calculate the probability of risks occurring in a government or the probability of a system being vulnerable?*
e) *Can the ontology be used to show the risks associated with resource sharing?*

To address the research question, there are four main areas of focus. This study is focussed on 1) the development of a conceptual framework 2) the formulation of the conceptual framework into an ontological framework 3) the development of a tool to support the use of the ontology and 4) the use of a case study.

1. The ***development of the conceptual framework*** in Chapter 6 is based on the theoretical foundation of the main aspects of the research. This was conducted based on hermeneutic literature reviews.
2. The ***development of the ontological framework*** in Chapter 7 is focussed on: Development of an E-Government ontology: this thesis presents a semantically rich ontology knowledge base of three main ontology modules composed of sub modules:
    a) E-Government module composed of (Service Providers, Service Receivers and EGov Services) modules;

b) Security Module composed of (Vulnerabilities, Risks, Threats) modules;
c) Assets composed of (Components, System, Infrastructures, Platforms and IT Service) modules.

Each of the ontology modules is defined in terms of its classes, subclasses, properties and related relationships. The definition of these properties and relationships is essentially used in expressing the status of a service in relation to the above-mentioned modules when evolution occurs. To develop the ontology, the Ontology Knowledge base was implemented from multiple sources and further modelled with the Web Ontology Language (OWL) modelling API. This was used in defining the ontology modules as well as instantiating them. The knowledge bases used in this research include information from the following: Common Attack Pattern Enumeration and Classification (CAPEC) (CAPEC 2015), which is used to study how hardware systems and the components that make them up are exploited as well as attack patterns in software and how weaknesses in software are exploited in the application design or implementation phase of a software; MITRE which was focussed on the risk aspect of the research; National Vulnerability Database (NVD) which was focussed on data related to vulnerabilities.

3. ***Development of a tool to interface with the ontology*** in Chapter 8***:*** The use of a tool that interfaces with the ontology is important because different stakeholders can run queries using simple drop-down buttons, check boxes or plain English and get results with the use of the rich medium the ontology provides.
4. ***The use of a case study:*** The case study involved contacting different stakeholders in government and discussing the effects of evolving services in government. The generation of data was through interviews, observation and analysis. The use of a case study was formulated with the help of scenarios which were developed in Chapter 7 and applied in Chapter 9.

1.3 Scope of Research

With respect to the research aims and objectives, the following delimitations apply:

a) This research focusses on only the risks of evolving services in government because different studies in government involving risks have been conducted (National Audit Office 2013b; National Audit Office 2011); risks involving government departments

(National Audit Office 2000); risks involving open government data (Kucera & Chlapek 2014).

b) This research does not discuss the aspects of risks and vulnerability analysis in terms of financial cost and therefore carries out limited study on cost impact ratings. This is not discussed because the results of this study reveal that costs are not static and may be for long term system and infrastructure operations and the financial aspect was beyond the scope of the research.

c) This research focusses mainly on soft infrastructure[17] especially on economic and social infrastructure. The research does not completely focus on hard infrastructure[18] because extensive studies on different types of hard infrastructure and their specific risks have been conducted (Little et al. 2012; Graham 2009; Kelly 2014).

d) Although this research focusses on ways of managing crisis as systems evolve which involves risk and vulnerability analysis, the research does not delve into the area of hazards considering that these are mostly accidental events that are non-man-made (Ragheb 2017). Therefore, the area of endogenous or exogenous hazards are omitted because during the research, findings from this study revealed that this could be problematic to analyse.

e) This research does not take into account that over extended periods of time, the state of a system or infrastructure may change and may give rise to new states which may impact the evaluation of the risk or vulnerability. The research focusses on just one active state of systems and infrastructures. Therefore, the time complexity of system change is not embodied in this research and all systems and infrastructures are assumed to maintain the same state.

1.4 Research Significance

The significance of the study is addressed in terms of advancing the theory of system and infrastructure evolution in government and with respect to risks and vulnerabilities.

It may also be of significance to key government stakeholders in the areas relating to providing joined-up government services and encouraging reuse across governments. This

[17] refers to all the institutions which are required to maintain the economic, health, and cultural and social standards of a country, such as the financial system, the education system, the health care system, the system of government, and law enforcement, as well as emergency services (Saftawy 2015).

[18] It refers to the large physical networks necessary for the functioning of a modern industrial nation (Saftawy 2015).

will prepare governments better for the risks associated with introducing and managing the application of technology in the afore-mentioned areas.

This thesis will contribute to the novelty of this research by using ontologies to analyse evolution risks. Complexities that exist across government departments as well as the effects of relationships in the form of dependencies and interdependencies in government will also be analysed. Also, the development of a prototype tool that interfaces with the ontology and answers questions relating to the reuse of assets as well as the complexities of merging or depending on other assets will greatly contribute to the novelty of this research.

1.5 Research Synopsis: Structure of Research

This thesis consists of ten chapters which are structured into five thematic parts. The outline of the research is presented in the following order:

Part I lays the foundation for the introductory part of the research in Chapter 1.

Part II consists of the theoretical foundation of the research.

Chapter 2 establishes the study in literature related to E-Government. Theoretical and practical practices in E-Government are presented to guide the research. A critical review of advancements, the challenges and risks associated with advancements in E-Government are discussed in this chapter. Chapter 3 discusses EGov Services as a subset of E-Government and the role of IT Services in the provision of EGov Services while Chapter 4 discusses the feasibility of the application of ontologies in E-Government as evolution occurs.

Part III consists of the Research Methodology and Framework.

Chapter 5 discusses the research methodologies which are used to justify how the research questions will be answered and the research process involved.

Chapter 6 presents the summary of the theoretical framework into the conceptual framework.

Part IV presents the development and evaluation chapters.

Chapter 7 presents the development of the ontology for the research using empirical case studies.

Chapter 8 discusses the development of the corresponding prototype tool

Chapter 9 discusses the evaluation of the tool and how the developed ontology supports the tool. It concludes with discussions on its applicability to governments using real world examples.

Part V presents the discussion and conclusion drawn from the research.

Chapter 10 concludes with discussion on the results of the research the quality of work presented, limitations of the research, recommendations and conclusions. It discusses the limitations; theoretical and practical implications of system change for governments. Possibilities of extending this research are also discussed in this chapter.

1.6 Research Publications arising from this study

During this research, some papers have been published in internationally recognised peer-reviewed conferences.

1. ONWUDIKE, O., LOCK, R. and PHILLIPS, I., 2015. Development of an e-government ontology to support risk analysis. IN: 15th European Conference on eGovernment – ECEG 2015, Portsmouth, 18-19 June 2015; Academic Conferences and Publishing International Limited; Pp 410-418
2. ONWUDIKE, O., LOCK, R and PHILLIPS, I., 2014. The use of ontologies to gauge risks associated with the use and reuse of E-Government services. IN International Data and Information Management Conference- IDIMC 2014, Loughborough, 17 September 2014; LISU, Loughborough University; Pp 56-67

PART II: THEORETICAL FOUNDATION

"*…This is a time to push forward, faster and on all fronts: open up the system, break down its monoliths, put the parent and pupil and patient and law-abiding citizen at the centre of it. We have made great progress. Let us learn the lessons of it not so as to rest on present achievements but to take them to a new and higher level in the future…. "*

-Prime Minister Tony Blairs Speech to National Policy Forum, July 2005

Chapter 2: Fundamental Concepts and Review of Literature relevant to E-Government

This chapter reviews relevant literature while defining the core concepts of this study so that a shared understanding can be achieved and ambiguity can be avoided in the reader's interpretation of the research questions and the work that result from this research. It also expounds on relevant literature providing evidence for the motivation of this research as well as the problems identified (introduced in Chapter 1). It starts with an overview of E-Government outlining the important concepts provided in definitions given by authors. Discussions on the different efforts made at achieving E-Government and the limitations of those efforts in current literature are presented. These discussions on the efforts currently being made as it relates to the risks of integration of similar services and assets, reuse, the methodologies currently being employed etc. are provided to set out the research questions.

2.1 An Introduction to E-Government

Electronic Government often known as E-Gov was established in the late 1990s and it was born out of the internet boom to transform manual processes to digital ones. The essence of its implementation at the time was centred on offering key government services online with the use of web portals. Before the 1990s, federal governments made use of information technology to automate backend operations without focussing much on the front end which involved the dissemination of information and delivery of services (Osterweil et al. 2007; Grönlund & Horan 2005). The focus at the time E-Government came into existence was on the internal use of IT within departments. However, it has evolved from a system of internal use to a system of internal and external use where the focus is on service provisioning (Dawes 2008; Seifert 2003; Al-Khatib 2009; Moon et al. 2014) while also focussing on the processes of the front end to the back office in ways that are modern and efficient (Government Digital Service 2017a). The definitions of E-Government are many and varied but one thing worthy of note in definitions given by most authors is that it is *focussed on the delivery of services*. To many, the promise of E-Government is to either *engage the citizenry* in government in a manner that is focussed on the citizens or to *develop quality government services* and *deliver systems that are more efficient*. The onus lies on governments generally to implement E-Government to improve the state of governance and delivery of services to her users by *eliminating processes* that *are inefficient* as well as *time-consuming*. EGov

Services are typically services that run using the internet as a medium where receivers of services interact with providers of services.

In a recent workshop held in London between members of the United States Digital Service (USDS)[19], 18F[20] and members of the Government Digital Service (GDS) in the UK, they concluded that although the operations of a government may vary in terms of political and operational circumstances there is a lot in common between governments. This commonality is ubiquitous to governments especially in the areas of public service provisioning and the needs of Service Receivers (hereafter referred to as SR) which appear to be very similar in modern democratic societies. They also reached a conclusion that governments largely operate in the same way except for policies which may be specific to individual governments (Mike Bracken 2015).

2.1.1 General Definitions and Views of E-Government

To complete this research, a working definition of E-Government is needed given that it is a contentious area which is subject to varying definitions. The aim of doing this is to formulate a framework conceptually to identify and characterise areas of risks in E-Government in relation to evolving EGov Services. To discuss areas of risks with the evolving nature of government, issues relating to E-Services, assets and stakeholders in government must be understood (Discussed in Chapter 3). However, before discussing these concepts, an overview of E-Government is first presented in this section.

Governments are constantly evolving and find themselves under enormous pressure to respond to change. The reasons for this may be because of how usable services in the private sector are perceived to be as well as high expectations from stakeholders in government. Responding to these changes mostly involve the transformation and digitalisation of processes in government especially with respect to government assets but more specifically government systems.

Digitalising government involves transforming manual and paper-based processes into digital ones with the use of the internet as an enabler which sometimes replaces the one-to-

[19] U.S. Digital Service is to deliver better government services to the American people through technology and designhttps://www.usds.gov/

[20] 18F is an office within the General Services Administration (GSA) in the United States of America that collaborates with other agencies to fix technical problems, build products, and improve how government serves the public through technology.
https://18f.gsa.gov/about/

one relationship government has with different stakeholders. This transformation may involve the restructuring of organisations in government as well as the systems within government. However, Weerakkody et al. (2009) argued that efforts towards transformations in government have largely resulted in the reinforcement of old practices and that changes which are more radical will be needed in core processes across organisational boundaries.

The introduction/inclusion of technology to E-Government is seen as an enhancer/enabler and in the words of West, **"***Digital is a necessity, not a "nice to have" technology"* (West 2016). As pointed out in 2.1, E-Government has evolved from a system of internal use to a system of internal and external use and this is because of its non-static nature. Based on most definitions provided by authors about E-Government, this thesis summarises this definition in terms of the value SRs expect to get from government in Summary Point No. 1.

Gupta & Jana (2003) viewed E- Government as a *necessity* and not as an option for countries whose aim is to *enhance governance* of her people. However, on a global scale, E-Government involves the *provision of opportunities* to *increase* the *connectivity*, *availability* and *interactive links* between various levels of governance and the citizen. Its development presents a way for governments across the world to *provide citizens*, *businesses*, and other *governments* with *convenient access* to *government services* and *opportunities of collaboration* as well as *political participation* via *internet* and *wireless communication technology* (Fang 2002; Keng Siau & Yuan Long 2005).

In recent publications it has been pointed out that in addition to the provision of services and increasing political/democratic participation, it should have as one of its objectives the *reorganisation of government agencies and the reduction of administration silos of information*[21](ReSPA 2015; KMD 2016; Gallo & Giove 2014; Ron Davies 2015; European Commission 2016). The reduction of organisational silos often requires a different kind of organisational structure to be efficient considering that the existent organisational structure may be historic and involve a number of paper-based processes (Service Futures 2015). This is summarised in Summary Point No.2.

[21] The reasons behind reorganisation and reduction of administrative silos include but are not limited to the following:
i.) the need to have an effective, efficient and accountable government delivered (Keith 2017; Pettypiece 2017); ii.) the need to eliminate financial waste in government (Washington Examiner 2017; National Audit Office 2012); iii.) the need to eliminate the complexity and redundancy that is seen to exist in government (Miller 2014); iv.) the need to eliminate overlapping responsibilities that exist among government agencies (The White House 2012).

Issues concerning improvement and advancement in E-Government are currently significant in E-Government research especially in the aspects of:

1. technology usage (West 2008; Ron Davies 2015),
2. improvement of citizen-facing services (United Nations E-Government Survey 2014),
3. use of innovative technology to identify gaps in government systems (The World Bank 2014),
4. Improvement of access to government through web usage (W3C 2009a).

This is still evident in the fact that like any organisation, E-Government is not static and therefore subject to change.

Mutula (2008) provided yet another way of viewing E-Government. He viewed it as an *efficient way of providing services* to citizens as opposed to the *traditional-based form* of government which he characterised as being *wasteful, involving duplication of files, manual physical filing systems* which he believed resulted in *loss of data* and the *inefficiency of government operations*. Mutula's view of traditional-based form of government can be likened to the street-level bureaucracy defined by Lipsky (1980) considering that the tasks of making decisions involving service delivery in both involve manual processes.

Naturally, the automation of a process with the use of technologies can be referred to as an automated or electronic process. Gil-Garcia (2004) referred to this automation of processes in government as *the use of information and communication technologies* to aid the *provision of public services, improvement of effectiveness of managers* and the *promotion of democracy*.

In 2001, Layne and Lee provided a definition of E-Government that became widely acceptable. They defined E-Government as the use of web-based technologies to *improve service delivery to citizens, agencies, employees, government agencies* as well as *make access to information owned by government readily available* (Layne & Lee 2001). Layne and Lee pointed out that the reason behind the establishment of E-Government was to *foster relationships with government* and the *public* so that citizens can effectively and efficiently interact with government (Layne and Lee, 2001). Hernon et al. (2002) tried to build on Layne and Lee's definition of E-Government by adding the need for 'access to service' thereby widening the scope of E-Government. They defined it as *"the use of technology, particularly*

the use of the Internet to enhance the access to and delivery of government information and services to citizens, businesses, government employees, and other agencies". According to Chen et al., (2006), *"E-Government is a permanent commitment made by government to improve the relationship between the private citizen and the public sector through enhanced, cost effective, and efficient delivery of services, information and knowledge".* Thus, this highlights the importance of establishing and understanding the relationships that exist between Citizens and SPs in Government. This is summarised in Summary Point No.3.

The results from conducting this research do not agree with these views because as much as access, delivery and improvement of services are important, these definitions do not take into consideration the present-day interactions that should take place between and within the government agencies that are responsible for the delivery of these services. Interactions as pointed out between Layne and Lee were between citizens and governments. However, interactions today take place between government, citizens, businesses, government organisations and even Third-Party SPs. Again, the definition of E-Government based on being web-based technologies might also be rather restrictive.

Barbagallo et al. (2010) explained that in line with the reason for its establishment, one of the main objectives of E-Government is the *development of solutions that are technological* which can *support interactions* between citizens and public institutions which would *improve public participation, social life* as well as serve as a *means for reducing cost.* Thus, the scope of E-Government has evolved beyond just service provisioning for citizens to more sophisticated levels (Goel et al. 2012).

2.1.2 Evolutionary Dimensions of E-Government

Anthopoulos & Manos (2005) pointed out that E-Government has evolved beyond the improvement of services. It has evolved from a *place of provision of services online* to a place where there are *systems, infrastructure and software that are reactive to the needs of citizens*; it has not just evolved but is being transformed considering the identification and authentication measures that are now put in place for a service to be transacted online. This has now become essential. Weerakkody et al. (2009) discussed this evolution in terms of transformational government (t-government)[22] pointing out that t-government evolved from

[22] "*t-government is the ICT-enabled and organisational-led transformation of government operations, internal and external processes, structures and culture to enable the realisation of citizen-centric services that are transparent, cost-effective and efficient"* (Weerakkody et al. 2009)

E-Government naturally. However, they argue that t-government covers a broader organisational and socio-technical dimension which E-Government does not cover which involves the radical change of operations, structures and the culture of government.

The views of t-government evolving from E-Government suggests that a variety of objectives need to be fulfilled in parallel to achieve E-Government. While there may be misinterpretations of the terms, they both have the same mission of providing better services.

At the time Layne and Lee gave a definition of E-Government, the web was still a growing technology. However, the web has evolved from version 1.0 of being a static web where there was limited user interaction and it seemed that governments were after asserting an E-Government web presence to version 5.0 where everything is now linked and intelligent (Flatworld business 2011). A borrowed term from the field of Systems Analysis makes use of the term "institutional lag" which demands that social systems should maintain the same pace with evolving technologies[23].

2.1.3 The Role of Technology in the Evolution of E-Government

In a policy paper delivered by the GDS in the UK, it was pointed out that digitalisation in government is simply not about interactions that take place online but fundamentally about the *internal operations of departments* (Government Digital Service 2017a). Beyond technological problems, Weerakkody et al. (2009) argue that the problems facing governments include strategic, organisational and social issues. This further explains that technology may affect processes in government in an exogenous way, however it does not totally take away the issues inherent in government since there are other dimensions to the problems that governments face.

Aldrich et al. (2002) pointed out that given that it is a constantly moving target, it is *not a stand-alone government effort* and *integration spanning across all levels of government* would need to be encouraged between government and citizens. While their focus on integration was between citizens and government, a survey conducted by the United Nations revealed that this target should not be a stand-alone effort of government but should be *embedded into wider socio-economic development framework*s (United Nations E-Government Survey 2014). Furthermore, a workshop conducted between the GDS, 18F,

[23] "*Today's public services must be designed with today's technology, to meet today's user needs"* (Mike Bracken 2015; Government Digital Service 2017a).

USDS revealed that the achievement of E-Government is a global effort; involving organisations and team effort (Mike Bracken 2015).

Meulen (2016) made a comparison between digital government and E-Government. He compared E-Government to Digital government as the number of services made available to citizens and the latter as a reduction in the number of discrete services in order to benefit from an integrated experience. Fountain likened the effect of this digital government to the economy by saying: *"Whereas dramatic efficiency gains and cost savings in the economy are rewarded through profits, promotions, stock price increases, and market share, similar gains in government are rewarded with budget cuts, staff reductions, loss of resources, and consolidation of programs* (p. 13) (Fountain 2001)."

Bracken recently pointed out that although significant cost savings may be made with the employment of technology, they are not the driving force or an end in themselves (Mike Bracken 2015). Arguably, technology offers a lot of benefits; however, there is the tendency to have utopian or dystopian ideologies of its applicability in government.

2.1.4 Understanding E-Government from the Aspect of Integrational Technologies

As stated in section 2.1.1, E-Government is a field that covers the economic, social and political processes involved in transforming the operations of a government. This thesis is focussed on the E-Government perspective rather than these other perspectives of government. Several authors have attempted defining E-Government in terms of Information science research and theories.

Ngulube (2007) defined E-Government in terms of it being a *phenomenon*. He defined E-Government as "*a phenomenon that is linked to the information society and the advantages associated with it*". He pointed out that the presence of E-Government allows *networking* between departments and the *integration* of their services is made possible with the *use of information and communication technologies*. However, Hasan (2015) argues that despite investments in integrational technologies, governments are still seen to *exist in cantons* with *limited* or *no exchange of data between them*. The use of information technologies is to improve service delivery as well as enhance the relationship between the public and government (Ngulube 2007). It cannot be denied that technology plays a pivotal role in improving service delivery. Generally, pundits may want to link the internet and the use of

technologies as providing an interlinked world and providing seamless service delivery; however, this is not always the case. The findings from this study agree that E-Government can greatly encourage networking between departments or government agencies but does not agree that the aspect of integration of services is completely true. This is summarised in Summary Point No.4.

There are many cases where integration of departments is in progress; there are also cases where these departments involved in the integration have no idea of what is going on with the department they are being integrated with[24]. However, this trend has continued over the years and Gillian Tett pointed out that one paradox of living in the modern age with modern and evolving technology is that there is a lot of *integration in so many ways* but in so many other ways there is also a lot of *fragmentation* and this is equally applicable in governments (Tett 2016). In a forward put up by Jochen Scholl, he argues that in many ways fragmentation may be purposive, but that purposive fragmentation should not cause systems in government to be dysfunctional. This is summarised in Summary Point No.5.

A recent report produced for the Institute of Government, Andrews et al. (2016) highlighted the problems associated with applying for a passport for a new born and the bureaucratic odyssey the parents/carers of the new born may need to go through. Their example was one elucidating the importance of technology and how it is possible to make each of the paper-based processes involved in getting this passport simpler, faster and cheaper[25]. However, the achievement of this is regarded as organisationally hard. The question is, are E-Government problems just hard problems, soft problems or a combination of both? While some authors argue that E-Government is designed from a hard perspective where the focus is on the technology, the processes related to the public sector as well as the data it handles (Parrado 2002); Gupta et al. (2003) argue that soft approaches are applicable in solving E-Government problems since they employ multidimensional attributes of information which are relevant in the E-Government context. However, Heeks (2006) argues that hard approaches to managing E-Government problems usually fail and that a hybrid approach to solving E-

[24] Fountain pointed this out saying that *"many organisational actors are scarcely aware of the potential of their technological systems. It is not surprising, therefore, that similar organisations may use* **identical information systems** *in vastly different ways…. The flexibility, decomposability, and functionality of the web and related information technologies mean that a system's objective characteristics may differ substantially from those that are actually used*". (p. 89) (Fountain 2001).

[25] In policing, paper work is the third biggest cost (Bracken 2015b)

Government problems is best fit for E-Government problems. An approach to solving these problems is summarised in Summary Point No.6.

Based on the different definitions and views of E-Government and despite the sometimes-conflicting expectations of stakeholders, the common denominator is that E-Government is supposed to meet varying objectives that sometimes conflict.

This section summarises with a working definition of E-Government for this thesis.

E-Government is the two-fold application of ICT-enabled technology in enhancing organic processes of government operations by creating opportunities for effectiveness, efficiency collaboration and interactivity while also using it to identify the gaps and risks created by the positive use of this technology.

2.2 Advancements in the Actualisation of E-Government

Several studies have revealed the enormous potential of E-Government. From the definitions provided by different authors, this thesis has provided a summary of its advantages. However, Section 2.3 discusses the challenges to the actualisation of E-Government.

1. Improvement and advancements of interactions that take place between citizens, businesses and governments (Andrews et al. 2016).
2. The provision of a single, joined up and integrated service which is estimated to lead to big savings. A typical amount of savings in the UK as cited by Andrews et al. (2016) is between £1.3 and £2 billion by year 2020.
3. Provision of better online services (Andrews et al. 2016).
4. Transformation of the way services are offered by a government leading to efficiency and the effectiveness of the government (Mundy & Musa 2010).
5. Automation of tasks that are manually undertaken by employees in government (Mundy and Musa, 2010).
6. Improvement of service delivery as well as enhancement of the relationships that exist between the public and government (Ngulube 2007).
7. The creation of new methods and avenues for participation in government (Jaeger 2003).
8. Administration is brought closer to citizens and businesses through the use of the Internet (Zukauskas and Kasteckiene, 2002)

2.3 Challenges to the Actualisation of E-Government

The essence of implementing E-Governments is to improve the delivery of services that a government offers to the users of the services. However, the complex nature of government is accompanied with various challenges. This section discusses the challenges governments face in the attempt to achieve successful E-Government.

2.3.1 Lack of Reuse in E-Government – A Multidimensional Approach

1. Lack of reuse of data: Organisations/Departments that are responsible for collecting government data often hold and solely use the data collected which makes reusing data and sharing information by legacy systems difficult (Government Digital Service 2017a). Data is seen as a component that is stored in different and frequently duplicated ways which makes it hard to have up-to-date data (Singleton 2015). Thus, government is still largely operating in silos since data is not readily shared across organisations/departments in ways that citizens would find comfortable. Also, a general approach to reuse is hardly ever employed in the development or distribution of the services being offered. This has resulted in a silo mentality across government. Summary point No.7 summarises how repetitive paper-based processes can be eliminated in E-Government.

2. Lack of reuse of Infrastructure, components and platforms[26]**:** Another limiting factor with E-Government is that there is currently hardly any reuse of similar components of a service; systems used to run the services and even resources across SPs which has led to the lack of integration that exists amongst SPs. SPs may not even be aware that reuse may be taking place across them which has led to a lot of replication in the E-Government domain[27].From recent studies, reuse is not being encouraged because some already developed business functions are found to be redundant (Kwon et al. 2015).

[26] Services are built on platforms.
A characteristic of services built on platforms is that they are more flexible (Singleton 2015).
[27] A typical example is seen in the production of over 300 licenses that required the same process but were delivered in ways that were completely different (Downe 2015).
Examples of systems which can be reused within government include: Distributed Authorization system which serves as an infrastructure for authentication, authorization, access control as well as auditing; the GOV.UK.Pay (Government Digital Service 2016) which is a payment system that is being used across government departments within the UK.

In attempting to encourage reuse, government departments encounter complications in reusing processes across government because different departments are found reinventing and re-procuring similar products even though they may be based on different standards.

3. Difficulty in finding code: The GDS identified that there is currently a lot of sharing of government code but little reuse because of the difficulty in finding it, it may be unsupported or it may be easier for departments to just start again by building their own (Government Digital Service 2016; Government Digital Service 2017c). If departments begin the process of building their codes, there is still the possibility of introducing duplicated code and duplicated services which does not make a government function effectively.

2.3.2 Challenges Associated with Silos

1. Silo Mentality and existence of silos: Silos arise in cases where suppliers of different systems or services become competitors. Not only is this an issue but there are cases of monopolistic competition where similar systems or services cannot be used as substitutes by other systems or services. The costs of having to switch to competing providers may cause problems especially if switching costs are significantly high and current providers are not meeting demands.

The existence of silos limit efforts targeted at reuse across government. The existence of silos brings about barriers which cut across different sectors of an organisation. However, if a culture that allows for collaboration and sharing in an organisation is enforced, there would be greater value and the silo syndrome would be reduced to the barest minimum. There are several silos that are in existence. Typical examples can be seen in the silos that largely exist in the NHS (Forte 2014; McCartney 2016; Michael Stewart 2014; Roux 2016; Walsh 2016b; Walsh 2016a; Weldring 2016).

The silo syndrome developed in organisations does not allow for interaction amongst departments. This can be seen in the E-Government domain where there is lack of integration amongst various SPs[28]. They make people focus on the specific mission of their department or agency instead of working towards a common goal. The impacts of having a silo mentality in any business or organisation are many and varied and this can be seen in the negative

[28] "*the manifestation of a silo syndrome is the breeding ground for insular thinking, redundancy, and suboptimal decision-making*" (Rosen 2010).
"The problem with silos is that they cause people to ignore the big picture and instead focus insularly" (Pattison 2006)

impacts they have on businesses. The development of silos within the E-Government domain leads to lack of interaction amongst citizens as data and resources become enclosed.

Recent studies on the Ministry of Justice in the UK revealed that there is a large proliferation of silos and even systems in government (Harbott 2016). Per Rosen, "*when people are culturally inhibited from interacting across departments and functions, they avoid sharing data and information outside of their silos. It's a vicious cycle, one that can cost an organisation in agility, productivity, and responsiveness*" (Rosen 2010). Pattison pointed out that the elimination of silos can be made possible if bridges across departments are created (Pattison 2006). These bridges may include some form of transformation. However, Bracken argues that even though transformations within government are encouraged, a siloed approach to it doesn't work (Bracken 2015a).

2. Duplication across governments: When silos exist, then there is decreased interaction which leads to collection of similar data across SPs. Again, there is the argument that duplication removes large single points of failure. In a recent publication by the GDS, it showed duplication, overlap and contradiction of datasets held by government (Government Digital Service 2017a; Korte 2014). Duplication is wasteful and even though some agencies often dispute that duplication is not wasteful based on the approach they have taken in their development (Korte 2014), eliminating duplicate services can potentially save a government large amounts of money and resources as well as eliminate redundancies and inefficiencies in government (Korte 2013; Graves 2013)[29].

2.3.3 Challenges Associated with Frontend and Backend Transformation

1. Transformation of citizen-facing services without transforming backend processes: while attempting to transform the interfaces that SRs interact with, there is lack of fundamental backend transformation. A typical example is seen where the front office and the interfaces service users interacted with met users' expectations but the processes and systems at the back end remained unchanged (Government Digital Service 2017e) and there have been no efforts to improve these internal services/processes (Government Digital Service 2017d). This is usually characteristic of legacy systems as they lack the convenience

[29] Citizens cannot afford to keep buying the same service twice or have their monies spent inefficiently (Korte 2013).

of modern interfaces but are still heavily relied on because of their mission-critical nature. This could presumably result in maintenance and evolution issues, wasted resources and working with an inefficient back end organisation. However, modernizing a system partially such as providing a rich user interface makes it more complex as ongoing maintenance of the system increases (Arkin Software Technologies 2016).

2. Integrating new technology with legacy systems: It may be difficult to replace legacy systems just because new technology is being incorporated because of the vital processes they handle within governments. A system may be considered a legacy system due to its inability to meet the needs of a business or to lack of support for the system (Altexsoft 2017). This makes it difficult to have other systems integrated with it considering its underlying architecture or general design. Maintenance and support may therefore be difficult when a new technology is added to a legacy system considering that a small update to the system to accommodate new technology might result in multiple conflicts. Faults that are developed with legacy software are a common reason for delays in providing services. Integration issues are also common problems that occur with modernizing legacy systems (Tibbetts 2012)[30]. While attempting integration with legacy systems, they can fail and in turn damage the credibility of the IT department. There may be more grave repercussions in terms of the security[31] issues this may generate[32] such as the risk of using unpatched software (Lamb 2008). There are also cases where services are developed on platforms that no longer apply and this separates the services from what makes them work (Singleton 2015). The flexibility of knowing what services or components to pull apart or bring together when platforms no longer apply is a challenge.

2.3.4 Challenges Associated with the Growth in Systems of System (SOS)

The concept of Systems of System or Systems within Systems spans beyond the Assets or components that make up a system but includes the connected, dependent and interdependent parts that make it up including the receivers and providers of the service associated with a system. A typical example of a SOS is the health care system which is made up of "*a set of connected or interdependent parts or agents—including caregivers and*

[30] *"companies run multiple systems and simply replacing one application...creates integration nightmares"*- Kimberly Harris-Ferrante
[31] "*The ability of a system to prevent unauthorised access to its contents" -(*ISEB 2010)
[32] maintaining security on legacy systems can be difficult, since users cannot expect automatic protection from new threats - John Lamb

patients—bound by a common purpose and acting on their knowledge (Institute of Medicine (US) Committee on Quality of Health Care in America., 2001)*".* Some of the challenges associated with SOS include but are not limited to the following:

1. Complexity Management: E-Government is characterised by complexity which can be attributed to the complex number of systems that are existent. Examples can be seen in cases where the back-office systems of a SP are integrated. Systems such as payroll, employee and accounting systems can be integrated to form a SOS. Although these integrated systems are developed to support the functions of government, they come with associated challenges. The question of managing these complex systems is of utmost importance considering that a combination of systems makes up an SOS and may require different procedures in managing them in the case of a crisis. Lane (2013) elaborates on the difficulty associated with managing crisis given that not all crisis makes use of the same system assets in order to resolve or manage a crisis.

2.3.5 Human-Related Challenges

1. Fear of transformation: Fear of transforming processes without changing the operations of the organisation because many departments have reached the limit of how far they can transform without major restructuring (Government Digital Service 2017b). The introduction of digital services to replace traditional/legacy ones may involve a transformation of departments approach to delivering services (Worley 2015). A leading cause of this fear may also be linked to the potential of job losses.

2. Lack of access: The lack of easy access to government services by citizens and stakeholders (Bhattacharya et al. 2012). Even with the objectives of the Freedom of Information Act FOI[33], FOI requests are not properly handled because of the existence of data silo infrastructures which makes compliance with requests difficult since they cut across departmental boundaries.

[33] The Freedom of Information Act 2000 provides public access to information held by public authorities by making public authorities obliged to publish certain information about their activities; and by allowing members of the public entitlement to request information from public authorities (ICO 2016).

2.3.6 Challenges Associated with Decentralisation

1. Decentralised services: Vassilakis & Lepouras (2006) identified different issues with E-Government such as the need to merge different EGov Services into one service and even the need to manage changes that may take place with doing this especially with respect to dependencies which may have cascading effects. Decentralisation may involve one service being delivered by different departments or agencies. A typical example is identified with the import and export service in the UK which is currently handled by 26 different government departments and agencies (Haberfield and Franklin, 2017). Their study revealed that this process is complex and the same cycle of duplicated data is evident in the processes. Decentralisation makes it difficult to manage all the services and more vulnerabilities and threats may be introduced to the system because of this.

2.3.7 Complexity-Related Challenges

1. Lack of organised information/data: A problem with E-Government as pointed out by Ngulube (2007) is the lack of properly organised information which may lead to the collapse of record management systems. Governments still have multiple storage of similar datasets which makes it difficult to understand which copy of the dataset should be relied on (Harbott 2016).

2. **Complex nature of Government**: One of the problems with governments is that they are very complex and there is no company that is faced with the amount of coordination of essential services and functions that a modern government is faced with providing (Government Digital Service 2017a). One of the reasons for this complexity stems out of the fact that different services are offered by different SPs with each SP operating on a separate budget. There are also complexities associated with the varying work procedures in government (Bhattacharya et al. 2012).

2.4 Advancement in E-Government and its Implications

The advancements in service personalisation and greater application of technology in the private sector have stirred the need for ICT solutions that are innovative. Therefore, a demand has been placed on governments to employ this same solution in the delivery of services to citizens (Mundy and Musa, 2010). As the economies of governments are being reshaped by the emergence of digital technologies, there will also be an increase in the efforts

being made to actualise E-Government. This may be characterised by free flow of information and data, quality platforms and infrastructure as well as the right skill set to drive innovation and deliver services that are critical to SRs. Governments are making efforts to actualise and advance E-Government and this section identifies some of the efforts that are being made and the implication of those efforts.

2.4.1 Attempts at Redesign and its Effects

1. Redesigning Services: According to Reynolds, this involves redesigning inefficient, entirely paper-based and outdated government services into cutting-edge digital ones. The aim of doing this is simply not aimed at digitisation of the existent service but to transform the already existent service into something good that people can readily use on the internet (Reynolds 2014).

A typical example is seen in the efforts made by the Government Digital service (GDS) in the UK to redesign the lasting power of attorney service[34]. The current system through which this service is offered is paper-based and it requires that a user enters their personal details e.g. Name and address multiple times on the same paper/form[35]. A prototype that was developed for this service revealed that the digital form asks for 70% less information than the paper-based form cutting down the number of forms to be filled from 14 (manually) to 4 (digitally). Abbott (2017) pointed out that "*the real opportunity for redesign lies not in simply improving the form, but the relationship around it".* In addition to redesigning services, the GDS added that the processes within government responsible for delivering these services need to be redesigned as well (Government Digital Service 2017b).

Downe (2016) views redesigning a service from a different perspective. She pointed out that it involves bringing together government services that are split into tiny pieces, products, content and isolated transactions provided by different parts of government and rebuilding them on the grounds of what services fit together. While Merwe (2016) views redesigning services as a move to orient the operations of organisations with a focus on end users, an Accenture transformation toolkit reported that redesigning has to take place at the backend for government services to be transformed (Accenture 2017) which the GDS reported is

[34] a service that requires that someone takes over financial and legal rights of someone else.
[35] This has proven inefficient because there is the tendency to get things wrong. Efforts to redesign this service involve building a product/prototype that will allow someone grant lasting power of attorney rights digitally (Reynolds 2014).

typical of most legacy systems in government where the interfaces were redesigned without a focus on the backend (Government Digital Service 2017e).

However, the GDS argue that current practices not only focus on the processes of redesigning the backend but also focus on the processes of the front end to the back office in ways that are modern and efficient (Government Digital Service 2017a). Holliday (2016) has a totally different interpretation for redesign, he focussed more on designing what is not visible to the public which include the fine, small details and the environment in which redesigning services take place while Christiansen (2015) pointed out that the focus should not only be on redesigning services but on the culture and functionality of a government.

2.4.1.1 Analysis of the Effects of Redesign

This thesis argues that although the existence of paper-based information flows as seen in the lasting power of attorney service have proved to be inefficient, analysis of using digital means to fill such forms have reduced duplication. However, redesigning a process based on analysis requires creative thinking which seem to have been applied in the redesign of this service. This thesis agrees with Abbott (2017) that the relationship around the improvement of forms should be the focus of redesign but argues that his definition of relationship is not explicit. However, this thesis is focussed on semantic relatedness. While services should be redesigned with user needs in mind, backend operations in view and the amalgamation of individual services; this thesis provides a new definition of redesign which includes that redesign is incomplete without the analysis of the effects it may have on ongoing operations.

Overall, there are a myriad of possible reasons for redesigning EGov Services, classifiable along the who, why, what dimensions. The different reasons for this can be quite complex and constructing an ontology taxonomy to model all these reasons would not be practical. However, the interest of this thesis in meeting the demands of redesigning services is in the risks associated with bringing these services together and the impact this has on the backend systems.

2.4.1.2 Analysis of the Effects of Redesign – Integrational and Relational Perspective

Redesigning services may require integrations and governments are currently involved in integrating systems and services but there are risks involved in doing this. For example, there are cases where systems are part of other systems and governments need to think of the

implications of the relationships[36] that they have. A typical example is seen in the Prison register which is *part of* the National Data infrastructure of registers (Vale 2017). Redesigning the prison service may require the integration of the prison register with another register. However, a point to consider when redesigning services is if a service ***is part of*** [37] other services or if the assets (Systems, platforms, infrastructure) that these services run on are part of other assets. Consequently, the ***has part relationship***[38] which is the logical complement of the ***is part of*** relationship that exists between these services or assets should be considered as well.

Redesigning a service may involve integrating a service with other services, analysing the ***is part of*** and ***has part*** relationships is important. In a statement published by the Public Administration Select Committee (PASC) of the UK Government, they indicated that all forms of arms-length government should be reviewed and a clear taxonomy of public bodies showing how each is governed and sponsored should be established because of the insufficient understanding across government on how government should work and who is responsible for what (PASC 2014b). This is testament to the fact that the UK government has no way of determining the existent relationship between departments and therefore cannot account for complex relationships or associated risks with this type of relationship.

Furthermore, in an attempt to develop a taxonomy for public bodies in government, a lot of inconsistency is seen in the use of language leading to confusion (PASC 2014b). This was acknowledged by the then Minister for civil society, Nick Hurd in this statement

"We are still left with an ecosystem of classifications and blurred lines between them that need further clarification" Q398 (PASC 2014a).

Again, there have been attempts at classifications within government, but of what use is a classification without relationships that exist between them. Furthermore, he pointed out that the system of government is filled with anomalies and anachronisms especially in identifying which public body performs a function[39] [40]. This statement makes it obvious that government

[36] The interactions that occur between entities. For example, Prison register is *part of* the National Data infrastructure of registers
[37] For this thesis, the is *part of* relationship is used to express part-whole relationships
[38] For this thesis and for illustration purposes for the *has part* relationship, this relationship is only used if an asset A always has part asset B as a part. Therefore, if Asset A exists, then asset B would always exist. But if Asset b exists, we cannot say for sure that asset A exists.
[39] "the system is full of anachronisms and anomalies". There are irregularities in what type of body performs which function, and in what they are called. Some bodies are classed as being of more than one type" Q404 (PASC 2014a)
[40] https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf

needs to be able to model existent relationships between service providing units in a way that captures relational semantics between concepts represented by the terms. The question of identifying which public bodies perform a function can be addressed with the use of ontologies because of their ability to be semantically enriched through the creation of many associations between existing E-Government terms using relationships specific to the E-Government domain. The implications of this for the thesis are summarised in Summary Point No.8.

2.4.2 Attempts at Integration

1. Integrating standalone services to provide more complex ones: As pointed out in Section 1.1, more examples of attempts at integration include: Attempts at integrating income tax and national insurance systems in the United Kingdom (House of Commons 2013). Attempts at merging the Inland Revenue and the HM Customs and Excise departments into a single tax-raising ministry referred to as HMRC (White & Dunleavy 2010); merging of several government departments and of government agencies (e.g. Job Centre and the Benefits Agency to create Job Centre+) (Prowle 2012).

Yet another example at attempting integration of standalone services between governments is seen in the integration of business registers across the EU. This was developed as one of the strategies for the digital market to allow businesses launch cross border services (Ron Davies 2015). This is an example of an approach to tackling problems that may vary across governments. However, the plan to consolidate single services into complex ones may be at risk of failure. Examples are seen in the attempt to merge all Britain's payment into one (Universal Credit) and the National Programme for IT (NPfIT)[41] which was aimed at integrating patients' records (Campion-awwad et al. 2014).

There are also attempts at designing and delivering joined-up end to end services which involves transforming the way government departments run and breaking the barriers that appear invisible but exist between these departments so that EGov Services can be improved for users (Government Digital Service 2017a; Harbott 2016). A typical example identified by Haberfield & Franklin (2017) was in discovering the processes involved in importation and exportation of goods in the UK as discussed in 2.1.2(11). Their study revealed that this

[41] https://www.cl.cam.ac.uk/~rja14/Papers/npfit-mpp-2014-case-history.pdf
http://www.nationalhealthexecutive.com/Health-Care-News/npfit-for-purpose

process is currently handled by 26 different government departments and agencies which makes the system complex and the same cycle of duplicated data as pointed out in 2.1.2 (4) is the case. However, Campion-awwad et al. (2014) argue that large IT schemes that are centralised and imposed on semi-autonomous schemes rarely work.

2. Integrating new services into large legacy systems: efforts are being made at rolling out new services onto already existing legacy systems which have been found to reduce time-consuming tasks. A typical example is shown in the 'visit someone in prison service' where family members of offenders can contact them digitally (Havelock 2017b). As pointed out in 1.1 new services are being added to legacy systems. Incorporating a new service to an already existing system is a good thing to do because it may be more expensive to roll out a new system, it may increase the positive impact of the system (Daglio et al. 2014). However, there are risks associated with adding new services to existing legacy systems. The existing system may be coming to the end of its life, integration of new technology with an already existing one may also prove difficult. There may also be the risk of failure when attempting this with systems that are complex (Havelock 2017b).

2.4.2.1 Analysis of the Effects of Integration Using Workflows

Efforts are being made at analysing, understanding and simplifying the current workflows that exist within government with the use of workflow software tools[42] which help to automate data-driven activities in government using technology (Napier 2013; OECD 2009; Bare 2017; Segarra 2016; Strammiello 2016). However, some authors have pointed out how the use of systems have disrupted the use of workflows and reduced productivity[43]. In a report, Thomson Reuters reported that despite the many successes of workflows, it is difficult to manage multiple platforms across workflows (Thomson Reuters 2013).

Although, a significant value of workflows lies in the potential of reusing them (as patterns) since sharing them makes them useful building blocks that can be combined or modified to develop new studies (Belhajjame et al. 2015). Previous studies have shown that *"storing workflow specifications alone is not sufficient to ensure that they can be successfully reused, without being able to understand what the workflows aim to achieve or to re-enact them. To gain an understanding of the workflow, and how it may be used and repurposed for their*

[42] Example of workflow software https://thinksmart.com/government-forms/
[43] A disadvantage of an Electronic Health Record System is disruption of work-flows for medical staff and providers, which result in temporary losses in productivity (Menachemi & Collum 2011).

needs, scientists require access to additional resources such as annotations describing the workflow, datasets used and produced by the workflow, and provenance traces recording workflow executions" (Belhajjame et al. 2015). The question to ask is if governments are reusing workflows or if they are just storing them. Even if workflows are shared across departments, there is no guarantee that they will be successfully reused considering that results of experiments showed that there is the possibility for workflows to suffer decay owing to the fact that they could not be understood, downloaded or executed (Zhao et al. 2012). This decay could lead to failure in the system. *"These failures were shown to be a result of one or more of the following issues: (i) Insufficient documentation. (ii) Missing example data. (iii) Volatile Third-Party resources- Many workflows could not be run because the Third-Party resources they rely on were no longer available (e.g., web services implementing their steps"*– (Belhajjame et al. 2015)

Recent studies have shown that the use of ontologies can help in preserving workflows (Goble 2016; Mikelakis & Papatheodorou 2012; Belhajjame et al. 2015) but of more importance in this research is to analyse the risks associated with the withdrawal of support by volatile Third-Party resources and the effects it has on workflows in government.

2.4.2.2 Analysis of the Effects of Integration Using Patterns

Another effort being made to join up services in the UK is seen in the use of service patterns because of increased interoperability it provides. It is believed that the use of service patterns would provide a template for how a particular type of service can be built with the use of components (Downe 2015).

Attempts are being made to build government as a platform to address the issues pointed out in 2.3.2. The phrase government as a platform was coined by Tim O'Reilly in 2010 to represent services that were developed independently in silos which were disjointed. It involves breaking down things into smaller parts or blocks with each part doing its own job (O'Reilly 2010). This makes it easy to connect them together as well as scale them up if there is an increase in demand. It is also easy to fix the service if one part of it breaks. Examples of platforms in use within the UK include: GOV.UK for publishing, GOV.Verify for identity verification (Bracken 2015a). While attempting to build government as a platform there is also a shift from monolithic services to microservices. Hence, there is a

move from systems that are huge and enormous to specialised systems that are smaller and modular (Harbott 2016).

However, a major drawback of attempts at integration is seen in integrated services not working together effectively. This is seen in a statement issued by the Department of Health in the UK where combining health services and care services didn't work well together and the risks that emanated from this[44]. This thesis argues that the failure of these systems to work together has been due to the absence of an ontological framework and this is seen in a statement issued on the lack of comprehensive governance which has led to efforts that are uncoordinated across central bodies and the Department of Health (National Audit Office 2017b).

2.4.3 Attempts at Automating Current Processes

1. Overhauling legacy content owned by government (Government Digital Service 2017a). While attempting to automate processes, there may be the need to overhaul legacy content**:** As in 2.4.2 (2), the risks of dependencies that exist between legacy content must be taken into consideration. It is important to note that legacy content may be toxic and there are risks associated with overhauling or decommissioning legacy systems. Recent studies carried out on the processes that take place in the Ministry of Justice revealed that a move towards microservices is looming as pointed out in 2.4.2.2. Thus, this may mean the decommissioning of some of the legacy systems (Harbott 2016). The risks associated with decommissioning legacy systems must be considered as governments move away from monolithic services to microservices. Of most significance to this research is being able to use an ontology to structure the kind of risks overhauling a legacy system may have on other systems in government as well as the impact it has on service delivery in a pro-active way considering that a report revealed that there is hardly a focus on the issues which could pose the biggest risks in government.

[44] "But these services often don't work together very well. For example, people are sent to hospital, or they stay in hospital too long, when it would have been better for them to get care at home. Sometimes people get the same service twice - from the NHS and social care organisations - or an important part of their care is missing" - (Department of Health 2015).
https://www.gov.uk/government/publications/2010-to-2015-government-policy-health-and-social-care-integration/2010-to-2015-government-policy-health-and-social-care-integration

2.4.4 Attempts at Reuse

1. Reusing data, components, systems and services across governments: Previously in the UK, every government service had its own way of doing things even though this was common to all other services. One of these identified common things was taking payment. This problem is currently being solved with the GOV.UK Pay[45].

Users were faced with a lot of difficulties with making payment and there was a lot of duplication and inefficiency across government as each department had to invent its own payment platform. Third-Party relationships are existent in todays globalized world and this is currently seen in the relationship government has with the Payment Card Industry (PCI). They are known to grow a business, but this comes with associated risks.

2. Finding duplicate lists of the same data/assets across government: Data needs to be drawn from a single source considering that it is used and reused by multiple government services (Vale 2017). Example of data that is used and reused across government departments is the Personal Data which is used to apply for a number of services such as: passport, driving licence, ordering a copy of a birth certificate, applying for benefits (Bolychevsky 2017)[46]. The data that government needs to deliver the right service does not all live within a department and this puts a burden on users since they have to provide the same information to different departments to prove their identity and eligibility multiple times (Bolychevsky 2017). To address this issue, efforts are being made to standardise the processes around the use of personal data[47]. One of the efforts that has been put in place to verify identities across departments in the UK is the GOV.UK Verify Service[48]. However, a problem with this is that central government has no standard way developed to verify identities because the GOV.UK Verify makes use of Third-Party identification companies who verify identities first before confirming a SRs identity to the department a service is being requested from. *"When your organisation relies on Third-Party suppliers or service providers, your exposure to risk multiplies"* (The Institute of Internal Auditors 2014). In addition to the issues raised in 2.4.4.1, this research is also concerned with how to manage relationship risks associated with third parties since they are often overlooked (Warren et al.

[45] A typical example seen is the GOV.UK Pay which is one payment system that allows for one simple convenient way of processing payments for every government service allowing users to pay for government services in the same way without having to pay for different services in different ways (Government Digital Service 2016).
[46] https://data.blog.gov.uk/2017/01/19/building-data-infrastructure-for-personal-data/
[47] i) by building trusted and reusable tools ii) automating and digitising existing services to reduce the time, cost and risks associated with recollecting, copying, storing and matching data.
[48] https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

2014) and the risks associated with the failure of Third-Party systems. Organisations are known to manage their Third-Party risks in silos (Davis 2015; Warren et al. 2014). Warren (2014) points out that "*when each business segment manages its own Third-Party risks from a silo, it's difficult, if not impossible, for a company to see all of its risk exposures".* Therefore, SPs in government need to be aware of the third parties' government does business with and identify the risks associated with this.

While attempts at managing Third-Party risks have been carried out using compliance frameworks and risk management tools some organisations do not have any systems or processes to monitor or manage Third-Party relationships (Asia Pacific Fraud Survey 2013). More interestingly for this research is the use of an ontology to help SPs know which Third-Party companies[49] pose the highest risk and what can be done to mitigate it.

Also, evaluating information assets and mapping them to the technology support they need can lead to savings since identified surplus technology can be decommissioned (The National Archives 2017). Therefore, it is important to establish the original owner or which department has responsibility for it and map accordingly. Currently, government departments rely on Information Asset Registers (IAR) to identify what assets are in place. This is usually a manual process[50]. However, an ontology is useful in finding out what assets are in use because ontologies can be layered on top of existing information assets (CSC 2011). Therefore, they are an enhancement to the already existent IAR and not a replacement.

2.4.4.1 Effects of Reuse – Third-Party Perspective

Although the government-wide platform for processing online payments in the UK has been declared compliant with the PCI Data Security Standards to take payments on behalf of public sector organisations (Wirth & Smith 2016)[51], the questions of What if? and How? need to be analysed in some way. There is currently a system in place that allows GOV.UK Pay to log everything that happens which in turn alerts them to focus on things that are not properly working. We cannot say that government wouldn't look into some of the risks to

[49] Knowledge of third parties would involve having a full inventory of contracts and agreements, the kind of relationships that exist between them and government, a catalogue of Third-Party risks (Krivin et al. 2013; Asia Pacific Fraud Survey 2013).
http://ww2.cfo.com/risk-management/2015/09/three-questions-managing- Third-Party-risk/
[50] http://www.nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf
[51] http://www.ukauthority.com/news/6391/govuk-pay-leaps-payments-industry-hurdle?utm_content=bufferdff90&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

determine whether the use of their Third-Party provider is trust worthy but organisations are generally known for assessing and analysing risks during the on-boarding process and after that they relax in doing this (MetricStream 2017). This may be applicable to governments as well especially when a rolled-out service is perceived to be functioning appropriately. This thesis argues that we should be primarily concerned with analysing the risks associated with using Third-Party[52] payment processors using an ontological approach as this will make things more transparent.

2.4.4.2 Analysis of the Effects of Reuse – Integrational Perspective

Governments across the world are even making attempts at reusing solutions developed by other governments. Example: The Parliament of Brazil is studying the possibility to reuse E-Government software solutions built by Estonia, including the software used for Estonia's electronic-ID. Also, attempts are also being made to reuse solutions in government. An example is seen in the "Find a prison service" in the UK attempting to reuse the prison register (Vale 2017). Attempts at reusing the prison register have failed because of the lack of standardisation of the prison register even though there have been attempts at drawing information from only one source. It was reported that 71 inmates were released in error[53] in the 2016-2017 financial year because of blunders in the system (Dearden 2017).

Considering that duplicate data can be maintained by different people or bodies as in 2.4.5.1, the authenticity of the data or source needs to be verified. This thesis makes the argument that there is need to preserve data in the registers used in their original format while capturing the provenance[54] of the records. While preserving the data in the registers, it is equally important to understand the relationships the data/registers have with other data so that governments can identify what departments are using what and the risks of reusing the data. More importantly, this thesis makes the argument for trust amongst organisations in

[52] Third-Party payments are money transmissions where the receivers of the money remittance order(s) are based in one country, but where settlement for the order(s) is made by the payment of an invoice to a beneficiary (often in another country) (HM Revenue and Customs 2014).

[53] "A prisoner is officially classed as having been released in error if they are wrongly discharged from an establishment or court when they should have remained in custody". Examples of errors can include misplaced warrants for imprisonment or remand, recall notices not being acted on, sentence miscalculations or discharging the wrong person on escort "(Dearden 2017).

[54] *''Provenance is a record that describes the people, institutions, entities, and activities involved in producing, influencing, or delivering a piece of data or a thing. In particular, the provenance of information is crucial in deciding whether information is to be trusted, how it should be integrated with other diverse information sources, and how to give credit to its originators when reusing it. In an open and inclusive environment such as the Web, where users find information that is often contradictory or questionable, provenance can help those users to make trust judgements"* (Belhajjame et al. 2013).

government that are involved in sharing data. Trust is established in 2 ways in this thesis: i) in the form of an organisation accepting data from another organisation and ii) an organisation forwarding data to another organisation.

2.4.5 Attempts at Sharing

1. Sharing of data and code: The impact of technology on the proliferation of data in government is commendable. Reusing data in government has gained popularity in recent times (National Archives 2014; Dekkers et al. 2014; Espinar 2014) and they are being used for a variety of reasons such as: developing reports, promoting efficiency and accountability, creating new platforms and tools, for solving problems, creating new services (Roy n.d.; Creative Commons 2010; McGregor 2012; Creative Commons 2011).

Sharing of data and code has made large and easily accessible datasets and databases more accessible but has increased the risks associated with large-scale data breaches (Thomas & Walport 2008). *"There are symmetrical risks associated with data sharing – in some circumstances it may cause harm to share data, but in other circumstances harm may be caused by a failure to share data"* (Thomas & Walport 2008).

In its report on the protection of private data, the Justice Select Committee[55] said: *"There is a difficult balance to be struck between the undoubted advantages of wider exchange of information between Government Departments and the protection of personal data. The very real risks associated with greater sharing of personal data between Departments must be acknowledged in order for adequate safeguards to be put in place"* (House of Commons Justice Committee 2008). Consequently, datasets[56] in government may not always be structured[57] or if they are, they may consist of uncoded elements which have no direct link to standard terminologies[58]. Information created by service providing organisations is on the

[55] https://publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/154.pdf

[56] *"A collection of data, published or curated by a single agent, and available for access or download in one or more formats"* (Berners-Lee 2006)
"Linked Data is about publishing and connecting structured data on the Web, using standard Web technologies to make the connections readable by computers, enabling data from different sources to be connected and queried allowing for better interpretation and analysis." (Berners-Lee 2006)

[57] *"The Information Asset Register is a live document, and the style of entries varies because text is entered by the individuals responsible for managing the assets – the Information Asset Owners, across the Department and its Executive Agencies"* (Department for Transport 2011).
http://webarchive.nationalarchives.gov.uk/20120817151306/http://www.dft.gov.uk/publications/information-asset-register/

[58] Tim Berners-Lee outlined four principles of Linked Data: i) Use URIs as names for things. ii) Use HTTP URIs so that people can look up those names. iii) When someone looks up a URI, provide useful information, using the standards (RDF*, SPARQL). iv) Include links to other URIs, so that they can discover more things.

increase and despite the size of the organisation, it is important to understand this information that is being collected so that it can be protected and exploited (The National Archives 2017). Even with techniques such as data warehousing and data mining, it is difficult to maintain and reuse semantically complex data extraction and transformation routines efficiently. The use of an ontology-supported approach to describe concepts relating to E-Government would eliminate such complex processes.

2. Sharing common platforms, components and business capabilities that can be reused across organisations. The GDS defined a common component as one that provides defined functionality and usually exists in one place. Thus, making it easily integrateable into a wider service (Government Digital Service 2017c). Typical examples are seen in the UKs GOV.UK Verify which is used for online identity verification; GOV.UK Notify (Government Digital Service 2017c) and even GOV.UK Pay.

The use of platforms makes procurement and use of Third-Party providers easy. This allows government change suppliers without departments making changes to their services. This is encouraged because services do not necessarily have to interface directly with a specific SP because of governments' ability to balance the load between different providers more easily. While encouraging the sharing of platforms, it is important to also think of how these platforms will be maintained.

2.4.5.1 Analysis of the Effects of Sharing Data

There are many cases where information sharing has proved useful. A typical example is seen in the sharing of information and datasets that take place in the Department of Transport between the DVLA, VOSA (the MOT certification authority) and motor insurance companies (Department for Transport 2008)[59].

Relevant to this thesis is knowing what data to share and when it may be a risk to share or not share it across SPs. However, it is impossible to build a classification of when it may be appropriate to share datasets and for this reason the principle of proportionality[60] may be more appropriate. Although reusing code can accelerate the development of services and efforts are being made by governments to share codes; the risks associated with doing this

[59] http://webarchive.nationalarchives.gov.uk/20120817154603/http://www.dft.gov.uk/publications/dft-sharing-information/

[60] Proportionality is a legal principle that allows (or requires) balancing between competing values (European Law Blog 2013).

must be analysed. The GDS pointed out that doing this does not secure the maximum benefit reuse has to offer but creates paths that are divergent with multiple number of maintenance streams (Government Digital Service 2017c).

2.4.6 Attempts at Carrying out Updates

1. Updating systems, processes and policies: There have been recent attempts at updating the systems, processes and policies that enhance the way a service is delivered. A typical example is seen in the way the service of helping people with court fees is changing in the UK (Fallon 2015). Current approaches to this are longwinded and complicated[61]. Attempts at digitalising this service still make the issue of processing applications a complex process since staff still have to refer to guidelines even though these guidelines are all in one place (Money 2016). While websites provide information which is good, aggregating this information for SPs is more important because this can be used to answer user queries or can serve as input to other applications. An ontological approach to this could be useful in interconnecting the information systems, managing context-aware systems as well as knowledge-intensive systems.

2.4.7 Analysis of the Use of Evolutionary Technology in Software Development

1. Agile development: development of projects in government are gaining more popularity with the use of agile methodologies[62]. The 11th annual State of Agile™ survey revealed that the rate at which enterprise agility is increasing throughout organisations is at an accelerated rate (VersionOne 2017). In 2010, there was a directive by the Office of Management and Budget (OMB) to federal agencies imploring them to employ *"shorter delivery time frames, an approach consistent with Agile"* when developing or acquiring IT.

The application of the agile methodology to software development is known to improve the success rate of software development projects (VersionOne 2015) especially in the areas of managing changing priorities, increasing the productivity of a team and the visibility of a project (VersionOne 2015)[63].

However, there are challenges with using agile methodologies for development in government considering the complexity of governments, the number and complexity of

[61] https://mojdigital.blog.gov.uk/2016/01/05/making-it-easier-for-staff-to-process-help-with-court-fees-applications/

[62] It is known as an alternative to the traditional waterfall model considering that it is difficult and late to make changes since the waterfall method only accounts for failure at the end of a process (Daniel 2015).

[63] http://www.agile247.pl/wp-content/uploads/2016/04/VersionOne-10th-Annual-State-of-Agile-Report.pdf

systems etc. Hayes et al. (2016) point out the challenges associated with the use of agile – *"The challenge now is to scale agile to work in complex settings, with larger teams, larger systems, longer timelines, diverse operating environments, and multiple engineering disciplines. In this report, we discuss the dimensions of this scaling problem in detail and offer advice on crosscutting themes that warrant your attention".* In summary, the processes in agile are not applicable for all projects, especially large-scale projects (Heath 2013; Bjarnason et al. 2011; West 2016).

Analysis from the application of this methodology on the transport department in government revealed that using the agile methodology requires greater collaboration between departments and agencies. Owing to this lack of collaboration is the existence of tension between current governance requirements on how projects making use of the agile methodology should be executed (National Audit Office 2013a). There are many possible reasons why agile methodologies are being adopted in government projects which are classifiable along the why, how and when dimensions. The different reasons for this can be quite complex and constructing an ontology taxonomy to model all these reasons would not be practical. Some government departments like the DWP are known for their incorporation of agile methodologies in the development of projects especially in the aspect of introducing welfare reforms (National Audit Office 2013a)[64]. Knowing whether a government department is ready for agile is important as there have been cases of failure. Examples of such cases of failure include: failure of the Universal Credit system using agile in the UK, failure of Siren and the failure of NPFit. The failure of the Universal Credit and NPFIT is attributed to an attempt at providing systems which required the software to unify different approaches to problems in an enormous scale (SAPM 2014) using the agile methodology[65].

Johnson (2015) argues that the failure of agile in the Universal Credit System is due to a failure of agile adoption as opposed to the agile development process while Ballard (2013) argues that the system was not developed to be agile and therefore it is difficult to make such

[64] More examples of the use of agile in government are found in the following government departments (National Audit Office 2013a)
i. Modernising the infrastructure for the MOT (Vehicle and Operator Services Agency)
ii. Modernising the Internet Booking System (Driving Standards Agency)
iii. Modernising HM Coastguard (Maritime and Coastguard Agency)

[65] Reasons for failure of agile project include: Company culture, lack of experience with agile methods (VersionOne 2016), lack of transparency in the case of the universal credit system, lack of communication between internal and external teams (Johnson 2015)

a complex system agile since most of their practices still involved the use of the waterfall model. Hill (2016) argues that the failure of Universal credit is due to lack of experience in agile working methods while West (2016) argues that government projects are just not agile enough. However, the Cabinet Office argues that the Universal Credit Department has not adopted an appropriate agile approach to manage the Universal credit system. There is a gap in literature in explaining what an appropriate agile approach is. Based on the different assumptions why Universal Credit failed, this thesis makes the argument that it lacked the ability to intelligently manage the software development processes and that agile should not be blamed for the failure of the project in government because most of these projects were not agile in the first place. Although agile methods have value in themselves, they shouldn't be a panacea for the growing fad.

Fourteen challenges were identified by the Government Accountability Office (GAO) in 2012 in the areas of adapting and applying agile methodologies in Federal Government. Their approach was focussed on the use of agile methodologies as an "add-on" to existing processes and models of operations (Mueller et al. 2015). Diego Lo Guidice identified that different measures of success are used by government agencies in adopting agile methods as opposed to the measures used by waterfall method which involved the use of pre-determined features that made it into the final product (Ravindranath 2016).

Different methodologies have been used in government to analyse the risks of using the agile methodology. One such method is the Readiness and Fit Analysis (RFA) which is used to uncover risks and create strategies for mitigation when new government practices are being adopted especially in the aspect of distributed governance.

The intent of this thesis is to map factors that influence agile projects in government based on the different phases and the risks associated with adopting agile methodologies in government projects especially large and complex ones using an ontological approach. Governments approach to handling of risks is summarised in Summary Point No. 9.

2.5 Chapter Summary

In this chapter, a working definition of E-Government was provided based on the varying views of different authors and schools of thought. It was demonstrated how these definitions helped to shape the research motivation with the discussions on the advantages, disadvantages and advancements in E-Government. More importantly was the discussion on

how most authors emphasized the use of technology as being responsible for the developments that occur in government.

This set the line of reasoning for a better understanding of the implications technology plays while advancing processes in government. Although a conservative pattern may be assumed by the reader, the examples have however provided the relative merits of the use of technology in E-Government. The implications of the knowledge gathered in this thesis is summarised in Table 2.1. Furthermore, this chapter has been able to partly answer RQ1 and RQ2.

Table 2. 1: Summary Point and Implication for Thesis

Summary Point	**Implication for Thesis**
1.	The value of E-Government is seen in its ability to eliminate inefficient processes and to deliver services on systems that are efficient
2.	It would be logical to conclude that efficiency would be encouraged when silos are eliminated. But the benefits, challenges that need to be overcome and the level of institutional change that needs to take place must be addressed.
3.	Attention should be paid to the kind of relationships that exist between the different types of SPs and the effect of the non-existence of such relationships/interactions.
4.	With the drastic technology-led changes in government, it is not sufficient to continue to increase the number of services that are electronically available without employing ways to integrate the increasing number of services.
5.	There may be cases where it may be better to have fragmented services in place because of the risks associated with integration.
6.	The knowledge of what systems have been previously developed and what systems are compatible for integration should provide a rationale for reuse within government.

7.	The elimination of paper-based activities in providing a service is only part of the causal pathway to eliminating repetitive processes in government. It needs to be paired with effective discovery of potential existing alternatives.
8.	Government needs to be able to model existent relationships between SPs in a way that captures the relational semantics between concepts represented by the terms.
9.	It is unlikely that government have methods for keeping records on risk aspects especially before major projects are initiated. Creating new paperwork or processes for each project especially each time leadership is changed may not be the best fit approach.

Chapter 3: E-Government Services and the Role of IT Services

In this chapter, IT Service is introduced to enable the reader to understand how EGov Services which are services that are provided by a government are made available. The chapter discusses how IT Services are instrumental to the provision of EGov Services and how IT Services rely on Assets for an EGov Service to be delivered. Furthermore, EGov Services are discussed as a subset of E-Government and therefore inherit the characteristics of E-Government as well. A relationship is established between Stakeholders, IT Services, EGov Services and the risks associated with the use of Assets in making EGov Services available.

3.1 Service: Meanings and Contexts

Several authors have provided definitions on the concept of service especially in relation to where it is situated in multidisciplinary research. BMS (2011) simply defined a service as an activity that is a ***value-creator*** as well as a ***benefit provider*** for customers at specific times and places while W3C defines a service as *"an **abstract resource** that represents a capability of performing tasks that form a coherent functionality from the point of view of provider's entities and requesters entities. To be used, a service must be realized by a concrete provider agent"* (W3C 2004b). The Information Technology Infrastructure Library (ITIL) which is known as the best practice framework for IT Service Management defines a service differently in Version 3. It defines it as "*a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks"* (ITIL 2011). However, the definition of a service is sometimes criticized by different authors for not being substantial enough or all-encompassing considering the various dimensions that a service may have (Firescope 2013; Agrasala 2011b). In the definition of a service provided by ITIL, the concept of Service Provider is missing. Thus, the capability of a SP to deliver the value implicit in the service is not clearly defined in this definition. However, this definition serves as a starting point for discussions on the application of services in government.

Due to the evolving nature of a service, various authors have provided various means of defining IT Services such as: defining it from the perspective of the types of Services provided by ITIL (Agrasala 2011b); in terms of a high-level categorization of service groups (Agrasala 2011a); in terms of the SPs responsible for the delivery of particular services

(Kaiser 2015). However, Watts (2017) provides a response to this issue of ambiguity of defining what an IT service is by stating that an IT Service should be defined in terms of IT Governance frameworks[66] such as COBIT[67] and ITIL considering that these frameworks can be used to effectively manage services.

3.1.1 IT Governance Frameworks

Organisations that have recorded successes have suggested that IT should be embraced in any organisation as a significant part of doing business (COBIT 2012). Thus, IT should be included within the governance and management of any organisation. COBIT and ITIL are generic frameworks that are useful for organisations of different sizes including the government sector because of their ability to provide a common business language for organisations and deliver services that are aligned with the goals of the business (COBIT 2012; Jacobs & Harris 2015).

For this study, the development of the IT Service structure is based on COBIT 5[68] and ITIL V3 frameworks since they are a collection of best practices on IT management. These frameworks are discussed to set the background for the design aspect of this research since they provide taxonomies of key terms used in the IT governance domain which can be adapted to meet the specifications of the design. Some generic terms are taken from these frameworks and applied to this research such as IT Service, Asset, Risk, Stakeholders, Service Portfolio Management etc.

3.1.2 Types of IT Services

IT Services play an important role in any organisation that is in the business of offering services and the management of the life of an IT service is referred to as its lifecycle. The

[66] IT Governance frameworks describe taxonomies of key terms used in the IT governance domain. These frameworks enable IT services to be managed throughout their lifecycle.

[67] Control Objectives for Information and Related Technologies, commonly referred to as COBIT, is a best practice framework produced by ISACA for IT governance and management

[68] COBIT 5 addresses the governance and management of information and related technology from an enterprise-wide, end-to-end perspective. This means that COBIT 5:

- Integrates governance of enterprise IT into enterprise governance. That is, the governance system for enterprise IT proposed by COBIT 5 integrates seamlessly in any governance system. COBIT 5 aligns with the latest views on governance.
- Covers all functions and processes required to govern and manage enterprise information and related technologies wherever that information may be processed. Given this extended enterprise scope, COBIT 5 addresses all the relevant internal and external IT services, as well as internal and external business processes

lifecycle of an IT Service describes the processes involved with the initiation and maintenance of an IT Service. There are different types of IT Services designed to meet the different needs of an organisation (All definitions of the types of service are gotten from the ITIL glossary of terms). However, although they have been investments of money and time in building online services in the UK, it is difficult from the current processes to find the application of ITIL. As efforts are being made to develop and design the Government Service Design Manual[69] in the UK, the use of ITIL is only mentioned once which shows that either there is a current gap in the way EGov Services are designed or that the Government Service Manual does not rely heavily on ITIL. Also, in current literature, there seems to be a misuse and misunderstanding of the terms 'E-Service' and 'IT Service' when the concept of providing services in government (which this thesis refers to as EGov Services) comes up.

3.1.3 Types of IT Services based on Service Groups

IT Services play a vital role in the delivery of any service. Furthermore, a change in the structure of an organisation would necessitate a change in the IT infrastructure which directly or indirectly would have an impact on the IT Service. Therefore, a change in government may involve the evolution of an IT service over time. Considering that IT Services belong to different service groups, a change in the structure of an organisation may invoke a change in the service group it belongs to. Thus, an IT service may evolve from one service group to another service group. For example, an IT Service may start as a core service and evolve to an enabling service as the demands of an organisation change. Since ITIL is based on achieving a stronger focus on services, this section starts by looking at the different types of IT services. The official ITIL V3 Glossary has defined three different types of IT services which are:

1) **Core Services**: an IT service that delivers basic outcomes desired by one or more customers. An example of a core service is the email service because it allows users send and receive emails.
2) **Enabling/Supporting Services**: A service that is needed in order to deliver a core service. An example can be seen in the infrastructure services that would need to be in place for the email service to function. The infrastructure service may involve setting up

[69] Helps government teams create and run digital services that meet the Digital Service Standard

assets (networks, servers or associated components) which would need to be in place for the core service (email service) to be used.

3) **Enhancing Services**: A service that is added to a core service to make it more attractive to the customer. Examples include adding features such as recalling emails, address look up etc. Although they may not be necessary for a core service to function, they add value to a core service.

More importantly for this research is identifying the IT Services that support the processes that take place within E-Government. Considering that the request or delivery of an EGov Service may involve different processes and activities, it is important to identify the IT Services that support the different processes. Suffice to say that an IT Service would support IT Service processes. These IT Service processes may require inputs to produce outputs. Thus, an EGov Service may require the successful execution of one (or more) IT Service(s) to deliver value. Defining these IT Services in terms of core, supporting or enhancing Services provides a form of criticality definition considering that the failure of a core IT Service at a given point in time may impact the business processes involved in Service delivery but the failure of an enhancing service may not necessarily impact the delivery of an EGov Service. This is summarised in Summary Point No.10.

3.1.4 ITIL IT Service Catalogue

Critical information is contained in the Service Catalogue which is made available to the IT department and the organisation. It contains generic information relating to all services that are provided by the IT Department and can be applied across all platforms, environments or geographical locations of any organisation. Table 3.1 contains a list of some generic elements of the IT catalogue adapted from ITIL glossary page. They provide insights on how IT Resources and Services can be better allocated to EGov Services thus, accelerating responsiveness to SRs. The intelligence provided by an IT Service catalogue helps to ensure that IT Services are closely aligned with the critical business strategies of an organisation (Shearin 2010). The IT Service catalogue thus sets a basis for the development of the business processes that are involved in the delivery of EGov Services.

Table 3. 1: IT Service Catalogue

S/No	Elements of the IT Catalogue	Description of Elements
1.	Service Name	This refers to the terms by which a service is referred to
2.	Service Description	The description of a service should be written in clear and easy to understand terms
3.	Service Availability	The times a service is available should be made clear in the service catalogue stating what times a service may not be available. Critical times a service may be unavailable should be listed in the service catalogue
4.	Service backup	The times for a scheduled backup should be included in the service catalogue. For example, incremental backup, full backup
5.	Service Owner	This is the person responsible for the funding of a service.
6.	Service criticality	An organisation is responsible for determining the criticality of a service. The criticality of a service is essential to the running of a service especially in cases where there may be a disaster. A service can have any of the following critical stages: Mission Critical, Business Critical, Business Operational, Administrative Services.
7.	Mission critical service	This type of service requires continuous availability. A failure or break in this type of service can be significantly damaging.
8.	Business critical service	It requires continuous availability, though short breaks in service are not catastrophic.

S/No	Elements of the IT Catalogue	Description of Elements
9.	Business Operational service	These services contribute to the efficient operation of a business and are available to only internal stakeholders.
10.	Administrative services	They are required for the successful running of a business.

3.2 E-Government Services

This section discusses EGov Services in relation to the principles used in ITIL V3 and COBIT 5. The application of these frameworks to E-Government and EGov Services provides a means to access the correctness, applicability and usefulness of IT. The inclusion of IT Services to the delivery of EGov Services can be regarded as one of the contributions of this research.

The provision of services in government have been implemented at different levels using different platforms and initiatives. Some of these platforms include SAGA which was put in place by Germany, e-GIF in United Kingdom, ADEA in France and FEAF in USA (Brusa et al. 2007; Karagiannis 2009). Although most of these initiatives have expanded in scope they were all geared towards improved service delivery. A study carried out by Capgemini revealed that service delivery has evolved from just the supply of services using the internet as a medium to government delivering services that are better in a more efficient and inclusive society (Capgemini 2006).

In this thesis, EGov Services are treated as a subset of E-Government because E-Government as a term goes beyond the provision of public services[70] by government organisations. Since this thesis discusses EGov Services as a subset of E-Government, they are prone to inherit the characteristics from the greater entity (E-Government) but are still discussed independently of E-Government.

[70] Public services are also known as government services

Featherman & Pavlou (2003) defined "*Electronic Services (E-Services) as* ***interactive software-based information systems*** *received via the internet*". Likewise, EGov Services can be defined as government services delivered using the internet as its medium of delivery. This thesis refers to them as those services occurring digitally in the government domain which are accessed by internal and external stakeholders.

Although there may be some confusion associated with the naming style of some authors who refer to EGov Services as E-Services or public service; for this research, this thesis replaces them with EGov Services.

EGov Services are services that are managed by different organisations in government or services that may be outsourced and delivered to users of the system electronically. However, in addition to the management of these services, The Commission on 2020 Public Services has argued that these services should be organised around individuals and communities. This implies that citizens must be put at the heart of public service organisation and should be in control of decisions that affect them which can have a number of benefits including the co-production of outcomes from these services (Dunleavy 2010).

Lindgren & Jansson (2014) put up an argument that for a public E-Service (EGov Service) to be understood, it must be done in terms of a three-sided object with three equal sides where the three sides are of equal importance. They presented the three dimensions of a public E-Service as (1) service, (2) electronic and (3) public. However, this thesis adds a fourth dimension by including the aspect of interactivity. The question is what is the usefulness of an electronic/public service if it is static and cannot be interacted with? This thesis attempts to fill this gap by including the aspect of interactivity.

3.2.1 E-Government Models and Frameworks

Various frameworks and models have been developed and adopted by governments to fit their situations which has resulted in a variety of Government Architectures (Janssen et al. 2013). Janssen (2012) described a framework in terms of a matrix that visualizes the relationship that exists between the various elements in each domain. Heeks & Bailur (2007) argue that the use of models to represent domains or areas of interest have greatly dominated frameworks that are highly theoretical.

SPs in government have been actively involved in the development of IT architectures and this is seen in the number of existing E-Government architecture frameworks that have been created independently. Gartner differentiates between private sector models and public-sector models. While private sector models focus on business relationships, public-sector models focus on the jurisdiction of government and the relationships that exist between agencies, departments, businesses and citizens (Schulman & Baum 2003). The relationships that exist between government stakeholders are different from the kind of relationships that exist between stakeholders and businesses.

However, some frameworks have been developed for E-Government which are used to model different aspects of government. Some of the frameworks include:

E-GOV which is a framework that is used to develop E-Government systems at the national level to ensure sustainability in developing countries. It is developed with key actors and principles which include government, local stakeholders and principles such as national ownership, stakeholder engagement and the balancing of roles which may be internal or external (Dzhusupova et al. 2011). This framework was validated in Afghanistan using a real-life project context which was focussed on addressing sustainability challenges. However, a formal evaluation framework is being developed in another country to assess the sustainability of the results obtained from the initial project.

Davis & Galbraith (2012) described a framework for events which was focussed on people. However, this framework focussed on the SR rather than the SP.

The SmartGov project was developed as a framework for EGov Services. The aim of the project was to specify, develop, deploy and evaluate a knowledge-based platform to assist public sector employees to generate online transaction services (Macintosh et al. 2003). Although, this project went through a pilot testing stage which was accessible using the Ministry of Finance's server, there are no further details on the continuity of this project or the application of its framework in current governments.

Keng Siau & Yuan Long (2005) provided a framework of E-Government which showed the different categories of government services. This framework defined the different categories of government services discussed in (3.2.2) and E-Government stakeholders but differentiated between the interactions and collaborations that take place between Internal (G-G and G-E) and External stakeholders (G-B and G-C). Although this framework has

widely been adopted by researchers owing to its qualitative meta-synthesis approach used in synthesizing different E-Government stage models; the range of E-Government has expanded beyond just service provisioning that was provided by this framework (Refer to Figure 3.1). However, this framework has provided the platform for most E-Government framework development.

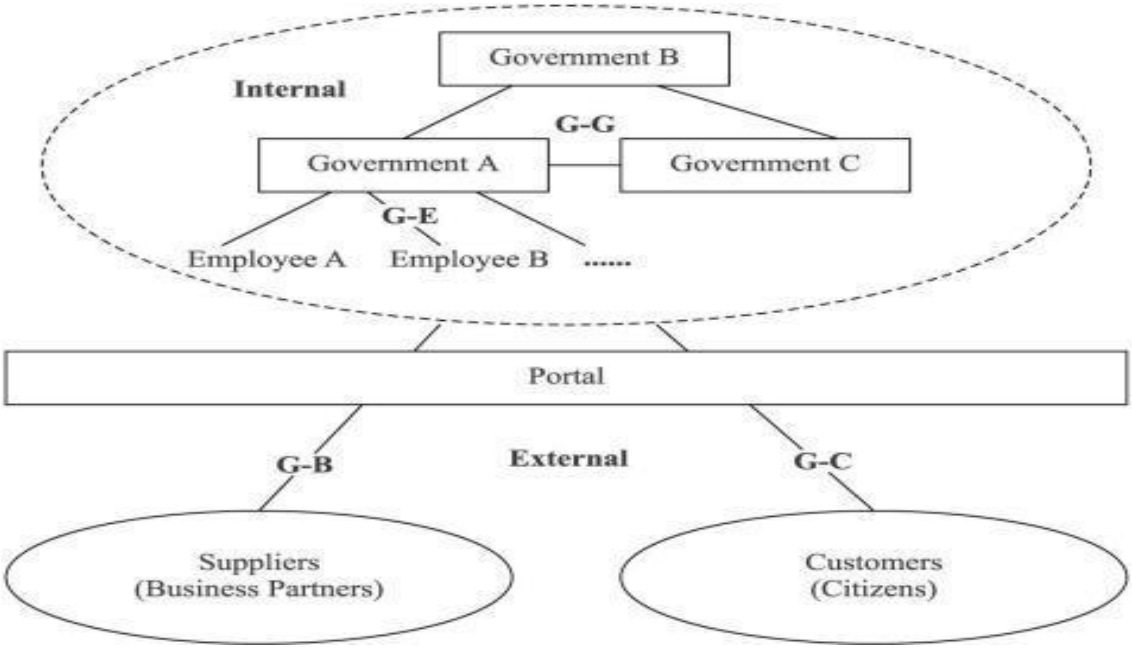


Figure 3. 1: E-Government framework diagram (Keng Siau & Yuan Long 2005)

3.2.2 EGov Service Categories

The EGov Services offered by a government differ according to the needs of users and this has necessitated EGov Services being broken down into different types. These services provided by government to her citizens can be viewed in terms of relationships and can be accessed at different levels of government.

1. **Government to Citizen (G-C)**: These are services that a government can and should provide to her citizens electronically. It should also foster the relationships that exist between government and her citizens and vice versa (Dudley et al. 2015). Examples include: Issuing passports, visas and permits; registering a vehicle.
2. **Government to Business (G-B):** These are services that a government can and should provide to businesses electronically. Wilmington (2017) defines it as a term that refers to the relationships between SPs and enterprises (businesses). Relationships that exist between government and business and vice versa are

strengthened by operations governments have with businesses. Examples include: Registration of a business; issuing licences.

3. **Government to Government (G-G)**: These are the services that the government provides to government organisations (agencies, department). It also indicates the kind of relationships that exist within government. Rouse (2010) also defines it as the sharing of data and /or information systems between departments, government agencies or organisations electronically. Services offered at this level include: sharing of data across government organisations, electronic management of processes. This improves data access, data sharing and communication.

3.2.3 Life Event

Based on the limitations of the processes involved in the delivery of EGov Services, the concept of integrating the processes is introduced and referred to as a Life Event.

The Information Systems Examinations Board (ISEB) defined an event as a behavioural thing that happens. It has the ability to create or destroy an entity which may affect several other entities or move an entity from one state to another in its lifecycle (ISEB 2010). The concept of a life event (hereafter referred to as LE) was introduced as a guiding metaphor for presenting and providing integrated public services. This thesis likens the processes involved in LEs as similar to those involved in Shared Services since it involves the integration of individual services into composite ones. This is summarised in Summary Point No.11.

Trochidis et al. (2006) defined LE as "*the inclusion of all public services that are related to a specific situation that citizens face"* while Ostasius et al. (2010) defined it as "*situations involving human beings that trigger public services*". For a LE to be delivered, it requires that a set of public services are performed (Todorovski et al. 2006). Ljupčo Todorovski et al. (2007) stated that LEs are tailored at helping citizens in identifying the set of public services they need at certain stages in life while providing a guide for the citizen.

For this research, LEs are defined as processes or activities that go on in the E-Government domain between a citizen and a SP. Examples of LEs include: registering the birth of a child, registering a marriage; applying for a driving license etc. Public services can be integrated to provide Les and LEs may also include a set of interconnected actions that a SR may need to take to receive a service.

Todorovski argues that although there have been attempts at modelling and analysing LEs, this is regarded as a demanding task because of the amount of time it takes to carry out the analysis which sometimes may lead to the production of inaccurate models (Ljupco Todorovski et al. 2007; Todorovski et al. 2006). These inaccurate models may be attributed to the use of inconsistent manual approaches. Again, more important for this research is to allow for queries that enable one to see the flow of activities within government and the use of an ontology is a viable tool for modelling this (Refer to chapter 4).

3.2.4 Challenges with Life Events

Considering that LEs are focussed on integrating services and providing joined-up services, there are various issues that come with providing them. Monroe (2015) discussed issues that must be considered before services can be pulled together to provide a LE which include: sharing of personally identifiable information (PII), issues relating to privacy, challenges with technology, agreement between SPs on areas of collaboration. These challenges can be linked to the implications of the advancement in E-Government discussed in 2.4.2 (1).

3.3 The Role of IT Services in the Provision of EGov Services

This research establishes that to provide or receive an EGov Service (child benefit service), an IT Service or a group of IT Services (Core Services, Enabling Services, Enhancing Services) as described in 3.1.3 would need to be in place. Furthermore, the software on which this IT service runs will need assets to run on. This is presented in Figure 3.2. There is a synergistic interaction that exists between IT Services and EGov Services. This thesis establishes the following roles in relation to the provision of EGov Services based on definitions of IT Services and EGov Services:

1. While EGov Services are services that are requested for and directly consumed by SRs, an IT Service is defined as a technical service or component that enables EGov Services.
2. Although IT Services may be used by SRs, they may only be used to access or enable an EGov Service.

3. EGov Services would be governed by Sersvice Level Agreements (SLAs)[71] while IT Services would be managed by Operational Level Agreements (OLAs)[72].

Based on this description, the following example is considered:

Applying for a child's passport in the UK (EGov Service) allows a parent or carer to apply for a passport for a child. This is made possible if the following criteria are met

1. an online application form is filled out to begin the process for obtaining the passport. This may require the use of an IT service known as IT Service Desk;
2. This EGov Service (passport applications service) can be consumed independently of other IT Services. Therefore, it may require an Email service (IT Service) for acknowledgement to be made using assets such as: Web server, fat client (computer), thin client, core server, smart client, rich client platform, middleware etc.;
3. Payment would need to be made using Payment Provider Services (IT Service) which rely on Payment assets to accept payment;
4. The confirmation email may require the use of a printing service etc.

[71] "A Service Level Agreement (or SLA) is the part of a contract which defines exactly what services a service provider will provide and the required level or standard for those services. The SLA is generally part of an outsourcing or managed services agreement or can be used in facilities management agreements and other agreements for the provision of services" (Cordall, 2012).

[72] An operational-level agreement (OLA) defines the interdependent relationships in support of a service-level agreement (SLA).

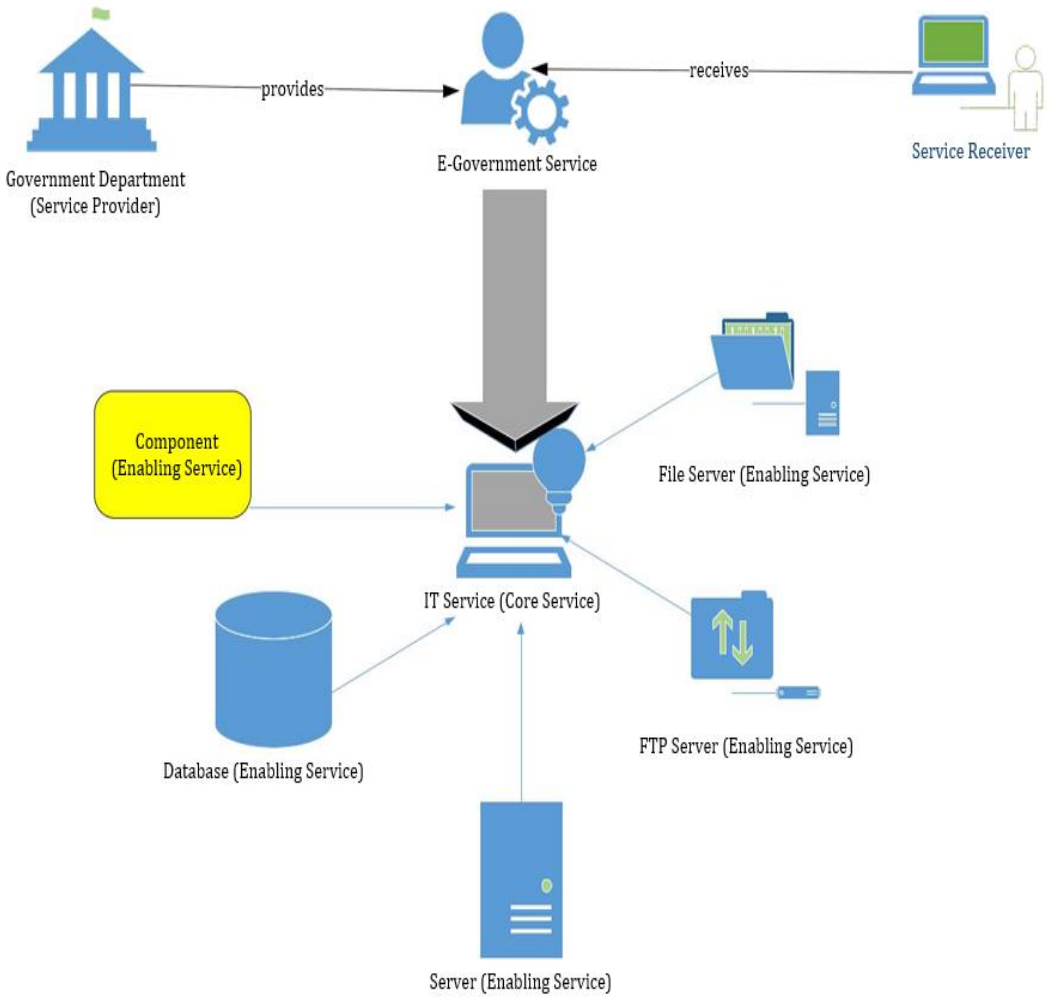


Figure 3. 2: Role of IT Services in EGov Services

Based on the description, the following relationships can be established for this research:

Every E-Government Service relies on one or more IT Services

Every IT Service supports at least one E-Government Service.

Based on the previous example, it can be said that:

The Passport Service (EGov Service) relies on multiple IT services which may include networking services, email service, a working device (computer, mobile, tablet) and the actual Passport Application Service which require assets (server, thin client) to run.

Therefore, if any of the components of an IT Service do not work properly, a SR may not be able to make use of an EGov Service. It suffices to say that an EGov Service is an aggregate of all the IT Services necessary for a service to be used by a SR and not just the application.

3.3.1 The Use of Shared Services to Transform E-Government

The Shared Services model is commonly used in the public sector because of the need to centralise and standardise transaction-based processes to ensure the efficient delivery of services (PWC, 2012). Making services sharable may involve transformational processes which come with associated risks and complexities. Although sharing services may provide opportunities for efficiency in government, no amount of this should set a government above the significant inroads that may be brought to bear.

The concept of Shared Services was introduced in the 1980s when the back-office operations of some large organisations were combined from separate units into a single unit (Redman et al. 2007). Numerous definitions of Shared Services exist in literature on this concept and varying terms are used as well such as *Shared Service Centre* (K. Hall 2016); *Shared Service* (Ulrich 1995); *Shared Service model* (PWC, 2012); *Shared Service Organisation* (Schulz et al. 2009). For this thesis, the term Shared Services would be used.

Bergeron (2003) viewed sharing of services as a management strategy where business functions that appear similar are consolidated within an organisation unit. Janssen & Wagenaar (2004) defined a Shared Service as *"a generic service that is jointly developed by public agencies and can be used many times in different business processes of various government agencies*. They outlined a list of generic services that could be made sharable[73]. This thesis builds on these sharable services and highlights the potential risks associated with making them sharable. This is discussed in Chapter 7. Other definitions which this thesis finds relevant include the definitions provided by Miskon et al. (2010) and Miles (2011). Miskon et al. (2010) defined shared services as "*the internal provisioning of services by a*

[73] 1. Communication service: the secure and reliable transmission of data and information between SPs and SRs with the use of a basic communication service
2. Message exchange service: uses communication facilities that are basic to transport and log messages from one system to another.
3. Identification and authentication service: This service can be implemented on various levels;
4. Authentic registration service: The principle of authentic registration states the organization who gathers the information at the sources, is responsible for keeping information up-to-date and for distributing the information to other organizations
5. Channel integration service: This facility is aimed at providing uniform and consistent service provisioning among various channels. Information about interaction on one channel is shared and used with the other channels;
6. Library service: This service aims at uniformly storing and making documents accessible in such a way that long-lasting availability and authentication of the document source is ensured;
7. Message exchange (specific) service: This aims at syntactically or semantically integrating messages within particular domains like taxes or social welfare;
8. Authorization service: This service should provide access to only authorized persons;
9. Business process integration: A set of services aimed at the coordination of processes across various organizations.

semi-autonomous organizational unit to multiple organizational units involving the consolidation of business functions supported by a sharing arrangement" while Miles (2011) defined it as "a*n organizational arrangement for providing services to a group of public or private sector clients via a service provider which replaces the previous in-house or contracted-out function*". This thesis focusses on some terms that are relevant to it from these definitions. Relevant to this thesis is understanding the types of risks that may result from consolidating business functions in government and the effects of the failure of a sharing arrangement based on Miskon et al. (2010) definition while also analysing the effects of replacement of previous in-house or contracted functions based on the definition provided by Miles (2011).

Furthermore, the interest of this thesis lies in the different aspects of sharing such as sharing platforms, functionalities, infrastructure and assets generally and argues that the scope of Shared Services should be widened to avoid misconceptions for researchers.

As with E-Government, technology is a significant enabler of Shared Services even though the focus behind sharing services is on the people and processes and the ability to do this using cost-effective means. The lack of reuse of functionality in development of services by SPs may encourage the existence of silos if services are not shared. As such the need for collaboration between SPs is important where services and functionalities can be shared.

There have been recorded successes with the implementation of Shared Services especially in the area of reducing cost, however there are also cases of failed projects where its implementation did not reduce cost (Farndale et al. 2009; K. Hall 2016; Dunton 2016)[74]. Voort et al. (2009) identified five potential benefits of using Shared Services [75].

Janssen & Joha (2006) argue that introducing Shared Services comes with associated complexities. In a report provided by IBM UK (2006), they argue that although the processes involved in providing Shared Services are difficult, there are benefits associated with doing this such as provision of better back-office services and a proven record of saving an organisation money. Leading organisations are seen to be challenging the inherent risks that may occur with sharing services, however, they are looking at ways to enhance the risk

[74] For example, the former department for Business, Innovation and Skills sank £14m in consolidating its legacy kit as part of a cross-government Shared Services plan that it later pulled out of

[75] Benefits of Shared Services: better service quality, reduced cost, enhanced transparency, building up and sharing of expertise and increased strategic flexibility

management practices while reducing costs (Ernst and Young 2014). Again, this thesis argues that reducing cost should not be the main driver for sharing services since the costs associated with risks may in the long run outweigh present cost savings.

3.3.2 Effect of Shared Services on Stakeholders

Two of the main reasons for introducing Shared Services are enhancing efficiency and reducing cost. Sharing services would potentially have effects on stakeholders in government. Some stakeholders may lose power, control and influence especially in the case where a single service is jointly developed by departments. Understanding the effects this has on the different stakeholders and their relationships is essential to this research. Voort et al. (2009) pointed out that introducing Shared Services may affect the outflow of staff leading to essential knowledge drain. The question is who manages these services if there are no longer staff with adequate knowledge.

3.3.3 Service Oriented Architectures (SOAs) in E-Government Shared Services

As discussed in Chapters 1 and 2, technology has been an enabler in eliminating efforts that are duplicated and there have been efforts at redesigning and improving EGov Services in ways that don't fossilise the old paper-based way of running government. Efforts to eliminate this duplication across EGov Services include the bringing together of individual E-Services to form a common service and this involves the use of Service Oriented Architectures (SOAs). As far back as 1998, The Parliamentary Office of Science and Technology (POST) discussed the use of technology in providing EGov Services that were joined up in a more holistic way. This involved grouping citizen and business services along the fundamental processes involved; grouping policy elements to serve more than one department and fusing these two groups together to bring an overall structure for government. The UK government began building SOA-based components and several web services in 2000 to enforce a whole of government approach to solve the problem of having disparate services resulting in duplicated systems and processes across government (Fishenden 2015).

Service Oriented Architecture (SOA) is a current and interdisciplinary field of research and its application in E-Government cannot be overemphasized. SOA (Jeong et al. 2009; Papazoglou et al. 2008) and Shared Services (Rolia et al. 2006; Tomasino et al. 2017) are

two areas of research that are entwined in the government and information technology field (Budhraja 2008).

Papazoglou et al. (2008) defined SOA *"as an architectural approach that utilizes services such as the basic constructs to support the development of rapid, low-cost and easy composition of distributed applications even in heterogeneous environments"*. Budhraja (2008) defined the adoption of SOAs as the foundation for facilitation between SPs and SRs while Behara et al. (2009) discusses an SOA approach in E-Government as the alignment of IT with service delivery goals which enables the reuse of developed assets by departments. Based on the reasons for the adoption of SOA approach in E-Government presented by both authors this thesis is concerned with the facilitation of relationships between SRs and SPs. Hence, Budhraja (2008) was not particular in his definition on what kind of facilitation he was discussing. Although the definition of approach provided by Behara et al. (2009) discussed the reuse of developed assets which is a major interest of this thesis, a limitation of this approach is the absence of accompanying risks. Therefore, this thesis builds on this approach to incorporate the aspect of risk and the evolution of assets in E-Government.

Saleh et al. (2013) stated that the main purpose of SOA is to promote services as the building blocks of functionality within applications and to allow a mechanism that allows simple access to this service via a web infrastructure while Budhraja (2008) discusses the advantages associated with adopting SOAs in government[76]. Budhraja (2008) summarises the effects of this adoption in Figure 3.3 below.

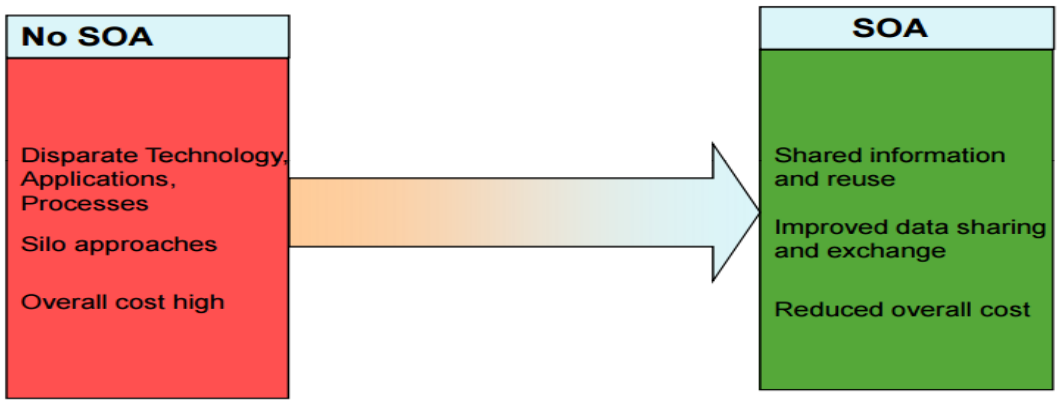


Figure 3. 3: Effects of Adopting SOA in Government Budhraja (2008)

[76] Benefits of SOA in government: promoting agility, reuse, manageability, productivity and adaptability.

According to Menascé et al. (2010), SOA's enable a multitude of SPs to provide loosely coupled[77] and interoperable services at different Quality of Service and cost levels.

Considering that departments are individually responsible for the development of their information systems; there is heterogeneity in the technologies and platforms used in the development of their services. The problem of heterogeneity can be solved using the SOA approach while trying to incorporate Shared Services. Saleh et al. (2013) explained that using this approach allows co-operation between systems that are heterogeneous since they are independent of the platform and the implementation language. Although, it has been established that better services and reduced cost are the results of Shared Services, BEA (2006) posit that departments require new ways of thinking about IT infrastructure in technical and organisational ways if SOAs must be implemented. The interest of this research lies in the new ways that SOAs can be used to deliver shared services and one of the new ways it uses SOAs is in the risks involved as integrations are used to provide better services and reduce cost.

Erl (2006) defined 9 key aspects of SOA principles presented in table 3.2. Column 1 contains the principles he discussed while Column 2 discusses how these principles apply to this research and the domain of discourse.

Table 3. 2: Application of SOA Principles

S/No	**Erl (2006) SOA principles**	**Application of Erl (2006) SOA principles to Research**
1	Loose coupling: relationships that minimize dependency and only require that services retain an awareness of each other.	The complexity of E-Government allows for a lot of dependencies and it is difficult to reach a conclusion where a change in one system would not affect another. From studies, the complexity of E-Government makes it tightly coupled. Assets on which EGov Services run should be loosely coupled so that if changes need to be made or components need to be replaced, this can be done independently.

[77] Loosely coupled services is a way to interconnect the components that make up a system or network so that the dependence between the components is to the least extent practicable (Rouse 2011).

S/No	Erl (2006) SOA principles	Application of Erl (2006) SOA principles to Research
		It may be difficult for developers in government to understand the entire system and all the interdependencies that exist. However, there may be the risk of duplication with loose coupling. An ontological approach to this will help in identifying whether it is safe to modify a component or system or asset.
2	Service contract: communications agreement, as described in service description	Communication Services provide new and improved ways to access a variety of services (Crown Commercial Service 2017). It enables the collection and analysis of several areas of a service and allows for standardised terms and conditions which are pre-agreed between departments. SLAs are also encouraged at varying levels between departments and the risks that occur when SPs don't meet up with their commitments. SPs understand what they are to offer and SRs also understand what they are to receive.
3	Autonomy: local control over the logic a service encapsulates	E-Government Systems encapsulate external services or systems and make them appear as local systems or infrastructures. A typical example is seen with the Third-Party providers used by Verify. UK. Understanding the logic which is used in encapsulating a service is important but more important is understanding the risks of the encapsulated service.
4	Abstraction: hides logic from outside world	E-Government Systems encapsulate external services or systems and make them appear as local systems or infrastructures. A typical example is seen with the Third-Party providers used by Verify. UK. The fine details of dependencies between third parties are hidden from the outside world.

S/No	Erl (2006) SOA principles	Application of Erl (2006) SOA principles to Research
5	Reusability: logic divided into different compassable services.	A number of EGov Services exist which can be combined to provide more complex ones, perform more complex operations or enact business processes. Understanding what E-Services are compassable and the risks involved in doing so is important.
6	Composability: services can be coordinated and assembled to form composite services.	EGov Services can be comprised of more than one component. Child E-Services can be contained within a parent E-Service. This research models EGov Services being composed of other EGov Services and models the risks associated with this. It also discusses the aspect of EGov Services forming service clusters. Service Clusters can be composed of atomic and composite services and focussed on jointly solving a problem with EGov Services. However, it discusses the aspect of EGov Services in relation to IT Services and the assets on which they run on being part of other IT Services or assets.
7	Interoperability: open standard-based interfaces and protocols for the plug-and-play architectural components.	Considering the number of silos that exist within government, the use of open standards would allow applications port from one platform to another. The application of this can help utilize skills instead of retraining staff. Open standards have been used in this research to ensure the reliability of information e.g. OASIS standards
8	Statelessness: services don't retain information specific to a particular activity.	In this research, the time complexity of system change is not embodied in this research and all systems and infrastructures are assumed to maintain the same state.
9	Service Discoverability: services can be discovered usually in a service registry	In this research, services are easily discoverable based on the Class of either IT Services or EGov Services and without the use of complex naming conventions

3.4 The Role of Asset Reuse in EGov Service Delivery

An asset as defined by the ISO/IEC 13335 is anything that has value to the organization (Bureau of Indian Standards 2009). An asset can be data, software, hardware, personnel, communications, services and they have values attached to them. These values that are associated with assets can be in the form of intrinsic or extrinsic values. RSA (2004) summarizes this value in their definition of an asset as *"a resource controlled by an entity as a result of past events and from which future economic benefits or service potential is expected to flow to the entity"*.

Government organisation units make use of assets and there is the possibility of reuse of these assets even across government units such as departments. Reuse is seen as a mechanism whose importance should not be ignored especially in the areas of increasing productivity and reducing the costs and time during the development of software (Da Silva et al. 2014). In the case of software development, source codes have been seen as the most commonly reused assets (Da Silva et al. 2014); there are other types of assets that can be reused across organizations as well as governments. This can include design models, business processes. Assets that are owned by any organization require management as well as maintenance. However, the maintenance or management of assets is dependent on what kind of asset it is that the organization possesses.

Assets can be classified based on who owns the asset. COBIT (2012) defines the owner of an asset as *"an individual or group that holds or possesses the rights of and the responsibilities for an enterprise, entity or asset, e.g., process owner, system owner".*

3.4.1 Types of E-Government Assets: The Role of Information Assets in E-Government

Information assets are used by organizations to increase competitiveness as well as increase the management of information assets; increase the use of professional knowledge which is used to achieve the goal of share and reuse (Li & Wang 2009). Knowledge about assets and their related management is dispersed across several types of documents such as books, papers, guides, patterns, standards etc. in different formats and with different levels of abstraction (Da Silva et al. 2014). For example, knowledge about reusable assets specification can be obtained in technical reports or books (OMG 2005; Ezran et al. 2002)

while knowledge about reuse repositories and reusable asset management can be found in standards, books and papers (Alvaro et al. 2007; Burégio et al. 2006; ISO 2008).

3.4.2 Managing the Effects of Reuse of IT Assets in E-Government

Since most organizations do not develop products that are entirely new at every stage of development, there is an increasing demand for the reuse of existing products and models. It is important to understand the concept of reuse especially with respect to reusing IT assets within government.

Sheng & Lingling (2011) identified information and data sharing as the cornerstone for E-Government. It has been established in preceding chapters that the sharing of Assets can bridge gaps as well as foster trust in the E-Government domain. Thus, the replication of data, information and resources across departments can be greatly managed if reuse is encouraged. In the case of reuse in government this thesis defines it as the development of similar applications by different departments where the likelihood of interaction amongst these applications is very limited.

The advantage of reuse is seen in the ability to foster relationships and interactions that exist especially in cases where there are similar developed applications. However, the challenges associated with reuse have been discussed in 2.4.4. While asset reuse may encourage the effectiveness and efficiency of government, it is important to establish what assets are likely to fail and the effects of failure especially if there is the potential that they would be reused.

3.4.3 Understanding Assets from a Systems of Systems Perspective

It is extremely difficult to find an individual security method; feature or technology that can survive on its own. There must be a place where it must fit into a larger system to prevent circumvention. This is one of the reasons that Systems being composed of other systems are in existence.

The concept of “System of Systems” (SoS) has emerged over the last decade. While the concept of “System” has more universal acceptance, the definition of “System of Systems” depends on the application areas and their focus (Dersin 2014). Although Boardman & Sauser (2006) collected over 40 definitions of system of systems from academic literature, documentations independently published by government, academia and industry and even

proceedings and presentations from conferences; no standard or universally accepted definition exists for this term yet.

SOS may be seen as an emergent class of systems which are built from components and are large scale systems in their own right (Maier 2006). DeLaurentis (2007) defined it as *''SOS consists of multiple, heterogeneous, distributed, occasionally independently operating systems embedded in networks at multiple levels, which evolve over time''* while Popper et al defined it as "*a collection of task-oriented or dedicated systems that pool their resources and capabilities together to obtain a new, more complex 'meta-system' which offers more functionality and performance than simply the sum of the constituent systems''* (Popper et al. 2004).

While some authors have defined SOS in terms of complexity such as the definition provided by Kotov (1997) *''Systems–of-systems are large scale concurrent and distributed systems that are comprised of complex systems''*; they can also be described in terms of the relationships that exist between them such as the definition provided by Baldwin & Sauser (2009) as *''an arrangement of independent and interdependent systems that deliver unique capabilities''*.

From the different definitions and uses of the term SOS, Maier (1998) implied that this term is related to a taxonomic grouping. To Maier, "it implies the existence of distinct classes within systems. Such classes are useful for engineering only if they represent distinct demands in design, development, or operation".

Another interpretation and definition of the concept of SOS was given by Maier. This definition involves the identification of five properties which is referred to as Maier's criteria (Maier 1998). Typical characteristics of SOS are highlighted from the definitions that have been given by (DeLaurentis 2005; Maier 1998; Maier 2006; Sage & Cuppan. 2001) and include the following:

a) operational independence of component parts: each system is independent and it achieves its purposes by itself. The disassembly of systems into component parts does not affect the purpose for which the component part was developed. If the SOS is disassembled into component systems of parts, these component parts must be able to operate usefully independently. In other words, a SOS is composed of systems which are independent as well as useful in their own right (Maier 2006).

b) managerial independence, i.e., each system is managed in a large part for its own purposes rather than the purposes of the SOS. That is to say that component parts or systems maintain a continuing operational existence independent of the SOS.
c) geographic distribution, i.e., a SOS is distributed over a large geographic extent. Thus, the geographic extent of component systems is large which makes it possible for components to readily exchange only information and not substantial quantities of mass or energy (Maier 2006).
d) emergent behaviour: the functionality and purpose for the development of a SOS is not resident in any component system i.e., a SOS has capabilities and properties that do not reside in the component systems. Emergent behaviours are not localised to any component system but is a property of the entire SOS (Maier 2006).
e) evolutionary development: the SOS is not a fully formed system. Its existence and development are constantly evolving with the addition, removal or modification of its functions and purposes (Maier 2006). Thus, a SOS evolves with time and experience.

Based on the criteria given by Maier (1998), Sage & Cuppan (2001) specify that SOS exist when there is a presence of a majority of the mentioned five characteristics. The definition of SOS given by DeLaurentis (2007) encapsulates the criteria specified by Maier (1998) and captures additional aspects, such as heterogeneity of component systems and multi-level structure.

3.4.3.1 Example of Systems of Systems

There are different examples of SOS that exist. The understanding that a government is a collection of systems is vital in this research. Some examples that are specific to government include the following:

Healthcare systems: These are systems that are very complex, diverse and distributed in nature. A healthcare system of systems (HSoS) can be defined as a collection of independent, large scale complex, distributed systems. HSoS exhibit operational and managerial independence, geographic distribution and evolutionary development (Wickramasinghe et al. 2007).

According to (Dale Compton et al. 2005). "*The health care system is the organization (e.g., hospital, clinic, nursing home) that provides infrastructure and other complementary*

resources to support the work and development of care teams and microsystems". The organization encompasses the various systems that are used in decision-making, information systems, operating systems, and processes (financial, administrative, human-resource, and clinical) to coordinate the activities of multiple care teams and supporting units and manage the allocation and flow of human, material, and financial resources and information in support of care teams within the health system (Dale Compton et al. 2005).

US National Airspace System (NAS): This involves several transportation systems that operate independently but share the same space and have no other choice but to cooperate.

Biometric System: this system is used to identify a person based on physical attributes

a) Infrastructure System
b) Educational System
c) Distributed IT System

Figure 3.4 presents a diagram to show how independent systems can be combined. In the bid to increase efficiency of processes, individual systems may be combined to form other systems which in turn may be critical to the running of a service. These critical systems may also be combined to produce one system. Managing the risks associated with SOS would involve understanding their individual components and how critical each component system is to the running of a service.

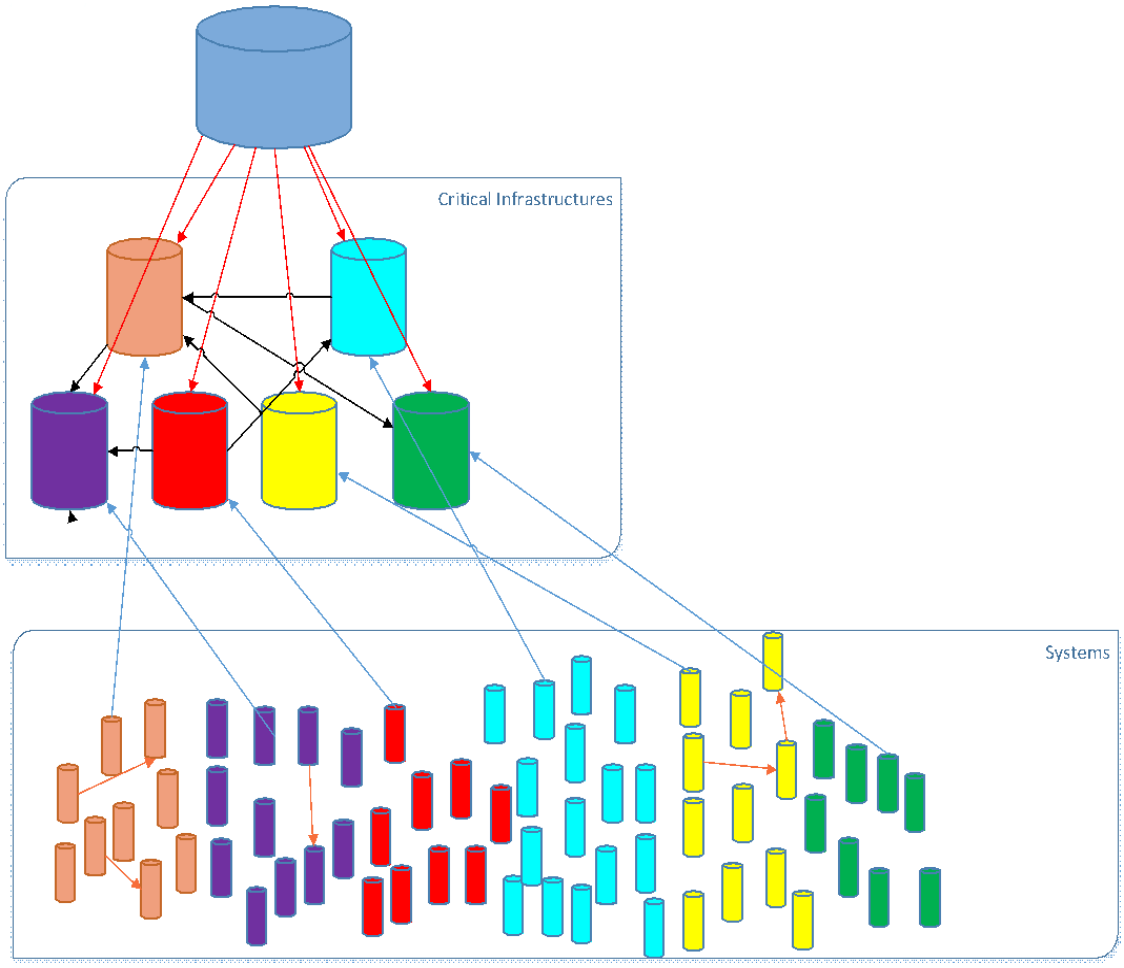


Figure 3. 4: Composition of Systems as System-of-Systems

3.5 The Concept of Risk Analysis in E-Government

The concept of damage is the starting point of any discussion that is held on the subject of risk and hazard (Kollarits et al. 2009). A risk is defined as the effect of uncertainty on objectives (AS/NZS ISO 31000 2009). It has the probability of significantly affecting the completion of major milestones adversely (Aked 2003). The ISO/IEC 13335 defines a risk *"as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization* (Bureau of Indian Standards 2009). Contrary to popular notions on its ability to be measured, this thesis takes the stance that a risk cannot be measured in units but can be evaluated relevant to other risks or based on defined criteria and the specific environment it exists in.

A risk that is not known cannot be managed (Proctor et al. 2008). Kollarits et al. (2009) defined risk management as a continuous process which involves processes that are aimed

at reducing risks to a level which can be classified as acceptable. They established that risk management is made up of different stages which include: identification of hazards; analysis of risks; evaluation of risks, treatment of risks and risk management evaluation. However, Robin & Uma (2011) define the management of risks to include the identification of possible problems and hazards; the evaluation of their importance in any given situation and the role they possibly play as well as the development of plans to monitor these problems.

Based on the processes involved as highlighted by (Kollarits et al. 2009; Robin & Uma 2011) and with the theory and analysis of risks in general, it is important to consider the motives for carrying out analysis, assessment and management of risks on assets within Government especially the risks that come with evolution; thus, the motives should guide the characteristics of the assets that need to be identified that may pose a risk.

As an organisation changes, there are evolution risks associated with this change and this requires a response in terms of risk priorities and policies (Proctor et al. 2008). This thesis adopts the method of managing risks proposed by Proctor which is shown as a set of sequential processes in Figure 3.5.

In a survey carried out by Deloitte, they pointed out that within the ISO55000 standard, risk management is seen as an indispensable aspect of asset management (Deloitte 2014). However, a review carried out on the organizational structures of a dozen companies worldwide and the reports produced indicated that the approach taken to manage risks are uneven and inconsistent (Proctor et al. 2008). Managing risks that may occur in a government must rely on a proper and encompassing risk assessment of government which reflects all assets used within the different areas of government that are possibly at risk. In a report released by the National Audit Office, it was established that Departments in government face challenges in developing an approach that is integrated and consistent to managing risks in a dynamic environment and, as such, approaches which are tailored to their own circumstances are likely to be the most effective (National Audit Office 2011). Thus, the need for a standard method of identifying risks that is accessible centrally within government may help to overcome this uneven and inconsistent approach.

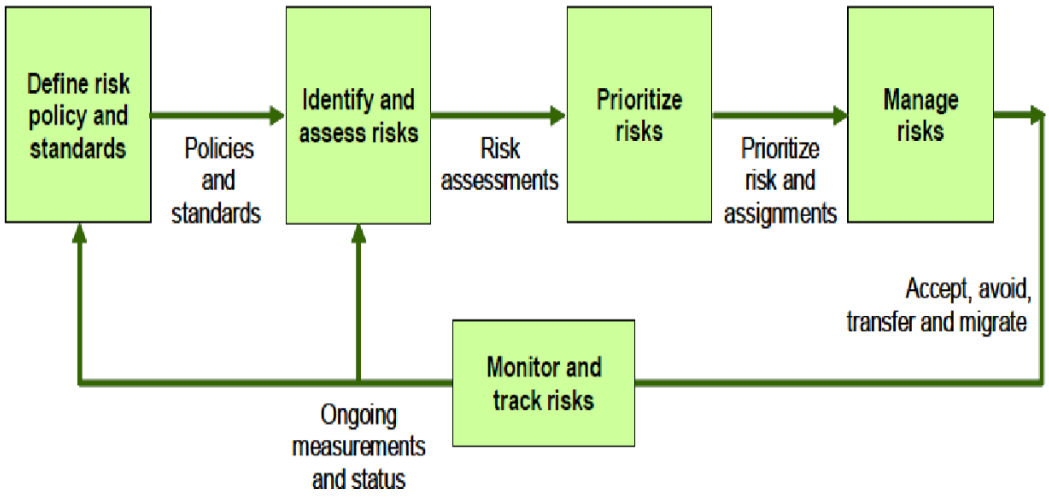


Figure 3. 5: Steps in the IT Risk Management Process (Proctor et al. 2008)

The use of a risk register has also been seen as a popular tool to aid the definition and management of risks (Saffin & Laryea 2012; Ray 2017; Chandana 2017). Webb (2003) defines a risk register as *'the most popular method of recording and ordering risks...specifying all perceived risks with the outcomes, likelihoods and countering strategies"*. They provide a means by which risks are logged and quantified based on the probability of their occurrence, impact or consequence which is usually expressed as Probability X Consequence. However, some authors have argued that expressing risks based on these two dimensions (probability and consequence) is an approach that may be insufficient in the management of risks (Laryea et al. 2007; Williams 1996). Saffin & Laryea (2012) argue that the aspect of financial implications and effects to the critical path should also be included because it enables the definition of risks in terms of time and cost. Thus, adding the dimension of focus to the risks as well as the related consequences.

Going by studies in fields like risk management, there is no standard register that exists which can be used in the recording and management of risks (The National Academies Press 2005; UK Government Cabinet Office 2011; The National Archives 2017b). The absence of a general risk register may be attributed to the fact that all domains are different and risk registers must be developed to adapt to individual domains.

Influenced by various authors, models and frameworks a risk register is developed for this research. Reiss (2007) lays a good foundation for the discussion on risk register which discusses the following: type and nature of the risk, impact of the risk and mitigation strategies to reduce the risk impact. RSM (2016) discusses the risk register in terms of the

different severity levels of a risk which are: high, medium and low risks while the National Risk Register in the UK typifies different types of risks, the likelihood of its occurrence (Cabinet Office 2008).

Risks to one sector of the economy or government can cause ramifications that may be global (Wyman 2009). Uncertainty regarding how risks begin and where they end has increased because of integration and interdependencies that exist in governments. A seemingly minor event such as the combination of services across government can as well become a full-blown problem as seemingly minor events may cascade into full blown crisis.

Approaches to managing risk in government have involved the use of different methodologies developed to meet a need and with different objectives. Examples include: Enterprise Risk Management (ERM) Systems (Hardy 2010); Rule-based models (Kaplan & Mikes 2012); project management approaches and audit frameworks employing the use of Failure Mode and Event Analysis (FMEA) and Fault Tree Analysis (FTA) (Aikins 2014); the use of standards such as ISO/IEC 27005 (ISO/IEC 27005 2011); the use of legacy suite of information on risks (National Cyber Security Centre n.d.); the use of asset-focussed methods of assessing and evaluating risks such as OCTAVE Allegro (Caralli 2007) etc. However, the impacts of a risk or the likelihood of its occurrence will not be diminished by the use of rules-based risk management (Kaplan & Mikes 2012). There are identified limitations with the currently used approaches to the management of risks such as inefficiencies due to overlaps in the treatment of shared risk (Hardy, 2010; Webster and Stanton, 2015). Also the use of some of the afore-mentioned approaches in the management of risks in E-Government show that it may be difficult to understand the cascading effect that exists between an organisation and the risks related to the objectives of an organisation (Webster and Stanton, 2015).

Although it is unlikely that any international standard for the process of managing risks will be created in the near future, there are a variety of existing application guides that are widely being used in different industries. Some of the standards include Guide to the management of business related project risk' the International Standard BS IEC 62198:2001, The British Standard BS-6079-3:2000 Project Management - Part 3, Project Risk Analysis and Management Guide produced by the UK Association for project management, Project Risk Management - Application and Guidelines, International Standard for Risk Management - ISO31000 - Risk Management. The combination of these risk management approaches with

an ontology will allow for the standard use of risk-related terminologies as well as the absolute use of measures as opposed to relative use of measures which could be a manipulative way of communicating risks.

3.5.1 Analysing Risks Associated with Interdependencies in Critical Infrastructures

Official descriptions of the word infrastructure are generally broad. Although most governments refer to physical infrastructure in their definitions, most of their definitions for infrastructure include assets that are intangible. However, in the United Kingdom, infrastructure refers to assets, services as well as systems. In Canada, their definition of infrastructure refers to networks, services, assets and physical and information technology facilities while in Australia, their definition of infrastructure refers to supply chains, information technologies, communication networks as well as physical facilities (Gordon & Dion 2008).

Infrastructures are regarded as assets. The report of the U.S. President′s Commission on Critical Infrastructure Protection (PCCIP), defines a critical infrastructure system as *"a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services"* (PCCIP 1997). These types of systems are mutually interdependent and highly interconnected (Robert et al. 2003; Peerenboom et al. 2002; Rinaldi et al. 2001). Some authors have tried to emphasize the enormity of importance behind critical infrastructures by defining it as the Central nervous system of a nation's economy (Yusta et al. 2011); other authors have defined it in terms of it being the supporting mechanism of any modern society (MacDermott et al. 2014).

The understanding that an Asset A_1 may provide support for another Asset A_2 while A_2 at the same time may be used to operate systems that are critical which are used in delivering a service is important. Therefore, it can be established with this statement that the failure of one Asset may have far reaching effects on an organization. The same applies to the failure of interdependent infrastructure.

Analysing risks of critical infrastructures proves to be a far more complicated task than carrying out traditional analysis. However, the information this analysis provides is important in the identification of vulnerabilities, preparing for emergencies as well as

prioritizing risks (Kjølle et al. 2012). In their research, they developed a bow tie diagram (refer to Figure 3.6) as a framework for analysing risks.

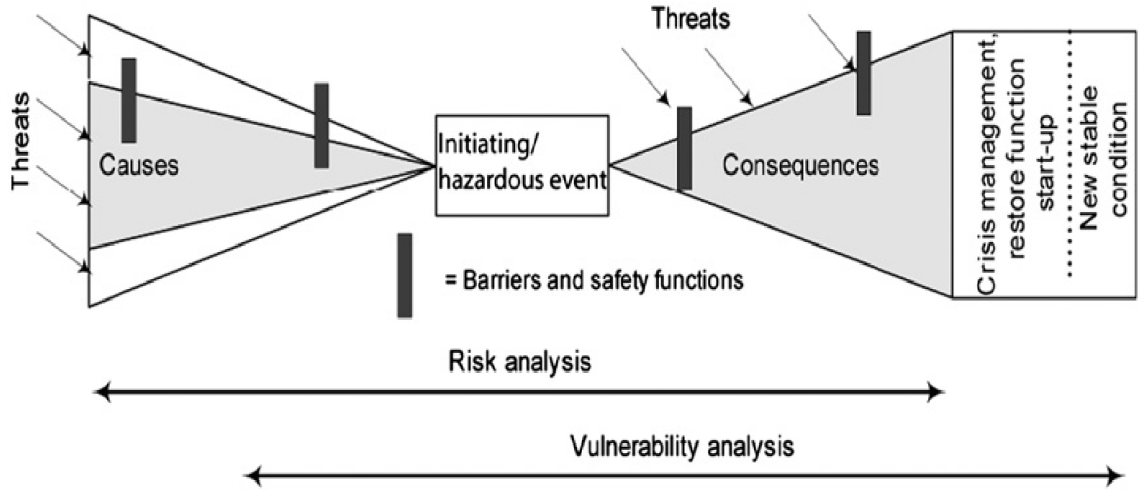


Figure 3. 6: Bow-tie Diagram Related to Risk and Vulnerability Analysis

The left side of this diagram represents the causes of hazardous events while the right side represents the associated consequences of the event. Vulnerabilities can be revealed based on the consequences and emergency preparation can be made (Kjølle et al. 2012). There is a tendency to focus on either the causes, consequences or both when analysing interdependencies. In this research, the focus is on both which is analysing the cause of a threat or risk and its associated consequence.

Burgess (2007) discussed the criticality of a critical infrastructure as necessarily negative. His description was based on the fact that critical infrastructures are analysed based on what may be lost or damaged. This may be a case where there is absence or loss of resources, services and facilities which may even occur across the different types of infrastructures that create their value in the effort to prevent their destruction.

3.5.2 Analysing the Different Critical Infrastructure Risks from a Security Perspective

Risk Management is made up of different branches and security happens to be considered as one of the branches of risk management (Arogundade et al. 2011). Security risk affects the value of the system in areas such as confidentiality, integrity, privacy, availability, and accountability (Arogundade et al. 2011). Consequently, increasing the security of a system is advantageous in various ways as the likelihood of events that decrease the productive

value of a system are combated. However, these advantages don't come without a cost which could be in terms of financial costs or decreased usability of the system. As pointed out in their paper, (Arogundade et al. 2011) stated that the use of the best security solutions is not always the highest but rather which serves as the best compromise between risks and cost.

In their paper, (J. Wang et al. 2010) adopted an ontological approach in capturing and utilizing the fundamental attributes of key components to determine how a systems security is affected by vulnerabilities. Although this ontology focussed more on Vulnerabilities, this ontology referred to as Ontology for Vulnerability Management (OVM) would be adopted in the development of the Vulnerability module for this research.

3.5.3 Analysing the Risks of Critical infrastructure of Heterogeneous Systems in Government

Studies have previously been carried out on the assessment of risks associated with critical infrastructures of heterogeneous systems. One such study is MICIE which was developed as a platform for online risk assessment in scenarios where there were heterogeneous interdependent critical infrastructures (Capodieci et al. 2010). According to Capodieci et al. (2010), critical infrastructures of heterogeneous systems are highly exposed to a large number of threats which include natural hazards, intentional attacks and even the failure of their components. These threats are as a result of increasing interdependencies between critical infrastructures which increases the effects of threats and challenges. In governments, not every system is made up of similar service components and therefore there is also a case of systems being made of components and infrastructures that are heterogeneous in nature.

3.5.4 Protecting Critical Government Infrastructures by Identifying Pathways to Risk

Although classical reliability theories such as the generic reliability model Grams (1999), fuzzy logic and chaos theory Rotshtein et al. (2012) have previously been used to model systems that are complex and large. Stochastic models such as the Markov and Poisson processes have been used to predict the behaviour of systems with uncertainties (Kotov 1997). Studies have shown that these methods of system prediction lack the capability to completely capture the underlying structure of the system and the ability of these systems to adapt to failure of subsystems when interdependencies that are stronger exist (Birolini 2014).

Critical infrastructures are seen to be heavily interconnected with a mutual reliance on each other which causes service provision to span across borders and even multiple countries (MacDermott et al. 2014). They are also very reliant on Information and Communication Technologies and owing to this reliance they have become highly interdependent (Rinaldi et al. 2001). They have different kinds of safety and security challenges in common. These include natural disasters, climate changes, ageing of systems, organisation restructuring, organisation outsourcing, terrorism as well as globalisation (NOU 2006). Albeit that a critical infrastructure is disrupted by a natural event or by a human-initiated action, the consequences of this can be far-reaching and may extend to other critical infrastructures potentially resulting in cascading effects that may impact all aspects of society (Bloomfield et al. 2010; Croope & McNeil 2011; Laugé et al. 2013). Considering that a subsequent disruption may increase the severity of an emergency, the importance of emergency management should not be overlooked while analysing critical infrastructures. This emergency management may involve the assessment of impacts of critical infrastructures and the ability to plan and prepare for emergencies (Klaver et al. 2015).

The breakdown of a complex network may escalate into an avalanche of component failures potentially leading to the complete loss of a critical service. Systems within government may be nonlinear[78] which is a characteristic of chaotic systems or linear[79] which is a characteristic of systems that may not be heavily connected and may be said to be good. However, the nonlinearity of these systems is evident in government systems and although initial failures may be independent of these systems, there may be more pronounced causal failure chains as time goes by which may lead to fully cascaded network of systems. Eusgeld et al. (2011) pointed out that SCADA (Supervisory Control and Data Acquisition) systems which are systems that are the backbone of industry may be a victim of these changes because it allows systems to adapt to changes.

Identifying pathways to risks may involve the following:

i. Identifying the types of relationships that exist between IT Services (for instance would an IT Service need to be fulfilled before another IT Service can be used).

[78] A system in which an output change is not proportional to the input change

[79] A system in which the systems typically exhibit features and properties that are much simpler than the nonlinear case

ii. Identifying the types of relationships that exist between EGov Services (for instance would an EGov Service need to be in place first before another EGov Service is provided.
iii. The impact an IT Service has on an EGov Service
iv. The relationships that exist between Assets (dependencies, interdependencies) and the effects of the withdrawal of such relationships.

Serious threats are likely to occur if there is competition for the use of critical infrastructures between the EGov Services and IT services that need them. Although, there is the likelihood that Infrastructures that are complex may be able to provide better services; however, this may increase the security risks and vulnerabilities. There has been a concentration of efforts by researchers in the area of modelling and analysing dependent infrastructures and a large focus on the structural vulnerability of single infrastructure (Crucitti et al. 2004; Albert et al. 2000; Albert et al. 2004) or interdependent infrastructures (L Dueñas-Osorio et al. 2007; Dueñas-osorio 2005; Leonardo Dueñas-Osorio et al. 2007). There are also several ways in which critical infrastructures are found to be dependent or interdependent. There is also an increasing dependence on sets of products and services which comprise of critical infrastructures. Considering that infrastructures are systems that are highly dynamical, the ability of an infrastructure to adapt to change in time is crucial to its ability to adapt to failures (Eusgeld et al. 2011).

Rinaldi et al. (2001) refers to dependency as a unidirectional relationship while interdependency is referred to as a bidirectional relationship. Although some of these relationships may initially appear invisible especially to the SRs, in cases where they are disruptive, they emerge and become obvious even to the SR. Although the issue of interdependency has been highlighted in different scenarios especially in scenarios relating to Physical infrastructures; this thesis adopts some of the definitions of interdependency provided by various authors and this is summarised in Table 3.3. These definitions provide links to scenarios (S1…. S10) and are adopted in the development of scenarios and modelling of interdependencies between assets in the ontology in Chapter 7.

Table 3. 3: Definitions of Interdependency in Different Research Materials with Matching Scenarios

Interdependency Type	**Definition**	**Scenario**	**Author**
Functional Interdependency	The operation of one infrastructure system is required and necessary for the operation of another infrastructure system	S1, S2, S4	(Zimmerman 2001)
	The functioning of one infrastructure system requires inputs from another system, or can be substituted, to a certain extent, by the other system	S1, S2, S4, S10	(Zhang & Peeta 2011)
Spatial Interdependency	It refers to proximity between infrastructures systems	S3	(Zimmerman 2001)
Mutual Interdependency	This is a case where at least one of the activities of each infrastructure system are dependent upon each of the other infrastructure systems	S4	(E.E. Lee et al. 2007)
Physical Interdependency		S1, S4	(Rinaldi et al. 2001)

Interdependency Type	Definition	Scenario	Author
	The state of one infrastructure system is dependent on the material output(s) of another infrastructure system		
	Some infrastructure systems are coupled through shared physical attributes. A strong linkage exists when infrastructure systems share flow right of way, leading to joint capacity constraints	S3	(Zhang & Peeta 2011)
	a physical reliance on material flow from one infrastructure to another	S4, S6	(Rinaldi et al. 2001)
	direct linkage between infrastructures as from a supply/consumption/production relationship;	S1, S4	(Dudenhoeffer & Manic 2006; Dudenhoeffer et al. 2006)
Cyber Interdependency	a reliance on information transfer between infrastructure	S2, S4	(Rinaldi et al. 2001)
Logical Interdependency			(Rinaldi et al. 2001)

Interdependency Type	Definition	Scenario	Author
	The state of one infrastructure system depends on the state of others via a mechanism that is not a physical, cyber, or geographic	S5, S6, S7, S8, S9, S10	
Input Interdependency	The infrastructure systems require as input one or more services from another infrastructure system to provide some other service	S1, S2	(E.E. Lee et al. 2007; Wallace et al. 2003)
Interdependencies due to policies	There is a binding of infrastructure components due to policy or high-level decisions	S5, S6, S7	(Dudenhoeffer et al. 2006)
Informational Interdependency	There is a binding or reliance on information flow between infrastructure systems	S2, S4	(Dudenhoeffer et al. 2006)
Shared Interdependency	Some physical components or activities of the infrastructure systems used in providing the services are shared with one or more other infrastructure systems	S7, S10	(E.E. Lee et al. 2007; Wallace et al. 2003)

Interdependency Type	Definition	Scenario	Author
XOR Interdependency	Only one of two or more services can be provided by an infrastructure system, where XOR can occur within a single infrastructure system or among two or more systems	S8	(E.E. Lee et al. 2007; Wallace et al. 2003)
Co-located Interdependency	Components of two or more systems are situated within a prescribed geographical region	S3	(E.E. Lee et al. 2007; Wallace et al. 2003)

Scenarios

S1: outages in power systems caused the failures of traffic signals, water supply pumping stations, and automated teller machines as well as the closure of businesses.

S2: disruptions on communication services affected the situational awareness and control of electric power (or water) systems and caused their partial failures due to lack of observability.

S3: water-main breaks flooded co-located utility systems. In the case of the World Trade Centre, the water flooded rail tunnels, a commuter station, and the vault containing all of the cables for one of the largest telecommunication nodes in the world.

S4: electricity loss led to the interruption of communication services (e.g., mobile phone services), which further affected emergency communication and restoration coordination of power systems.

S5: during the restoration process, the electric power systems and the communication services were usually given repair priority relative to other infrastructure systems and received more investment for improvement and retrofit.

S6: outages in power systems led to price changes of food and fuels.

S7: emergency services distribute emergency resources to restore various types of damaged utility systems. In the case of the World Trade Center, the New York Waterway with 24 boats dispatched some to work as floating ambulances from piers in Lower Manhattan and others to go to Hoboken, Hunts Point in Queens and the Brooklyn Army Terminal.

S8: debris-covered streets could not be used by both emergency response personnel and financial district workers, and lack of the latter could disrupt the financial services.

S9: most gas stations unable to pump fuel made drivers scramble to find functional gas stations, resulting in traffic congestion.

S10: closure of some metro stations increased the traffic load of the bus transportation system, resulting in long line ups at bus stops.

3.6 Analysing the Vulnerability of Assets from a Security Perspective

Wang & Guo (2009) defined a vulnerability as a security flaw, which arises from the design of a computer system, its implementation, maintenance and operation. They also referred to a vulnerability as a defect or mistake in a software which can be exploited by a hacker to gain access to a system or network. The study carried out by Elahi et al. (2009) attempted to define a systematic way for linking security knowledge by identifying basic concepts that play important roles when security issues are being faced. This study forms a core part of this research and would be adopted in the security module of the ontology since issues of security are issues that shouldn't be ignored.

Vulnerabilities are seen as "*weaknesses in the requirements, design, and implementation, which attackers exploit to compromise the system*" (Elahi et al. 2009). Elahi et al. (2009) identified the basic concept for modelling and analysing vulnerabilities and the effects they may have on a system. Identification of vulnerabilities and the ability to explicitly link them to the activities or assets that introduce them into the system is important because it enables analysts to identify vulnerable components within a system (Elahi et al. 2009). Not only are

vulnerable components within a system identified, the spread of vulnerabilities can also be identified; security failures can be traced with the aim of identifying source of vulnerabilities as well as affected stakeholders.

3.6.1 Analysing the Vulnerability of Assets (Critical Infrastructures and Systems)

A vulnerability as defined by the Bureau of Indian Standards and the International Organization for Standardization 27002 refers to *"A weakness of an asset or group of assets that can be exploited by one or more threats"* (Bureau of Indian Standards 2009; ISO/IEC 27002 2005) where an asset is anything that has value to the organization, the business operations and their continuity including information resources that support the organization's mission. It is also the absence of a proper safeguard that could be exploited by a threat (Fenz & Ekelhart 2009).

Vulnerabilities can also be defined as *"a flaw or weakness in the design, implementation, operation and/or management of an infrastructure system, or its elements that render it susceptible to destruction or incapacitation when exposed to a hazard or threat or reduces its capacity to resume new stable conditions"* (Johansson et al. 2011). This term is related to attacks and can also be described as the decrease of efficiency after the occurrence of an attack. The subjection of infrastructures to attacks decreases their efficiencies and increases the chances of the analysis of their vulnerabilities (Ouyang et al. 2009).

Although some pieces of work have collected and organized vulnerabilities in order to provide precise security knowledge to analysts (Landwehr et al. 1994; Avižienis et al. 2004); they however do not provide a conceptual framework that has enabled security requirements to be identified by analysts according to the identified vulnerabilities (Elahi et al. 2009). Studies have however shown that vulnerability of different types of infrastructures cannot be ascertained through their topologies. This has forced researchers to study vulnerabilities related to the functionality of infrastructures.

A methodological approach to modelling vulnerabilities was developed by Ouyang et al. (2009). This was developed so that the vulnerability of interdependent infrastructures can be effectively analysed. This approach which they used is adopted in this research in analysing the vulnerability of the different interdependencies that exist within Assets in government. This approach is represented in Figure 3.7 and involves the following steps:

1. Extract topology of each infrastructure which involves describing the nodes and the relationships that exist between them
2. Model the interdependencies that exist between the infrastructures
3. Analyse the structural vulnerabilities that exist between interdependent infrastructures by using the existing extracted topology
4. The functional vulnerabilities are based on the operation of each of the infrastructures.

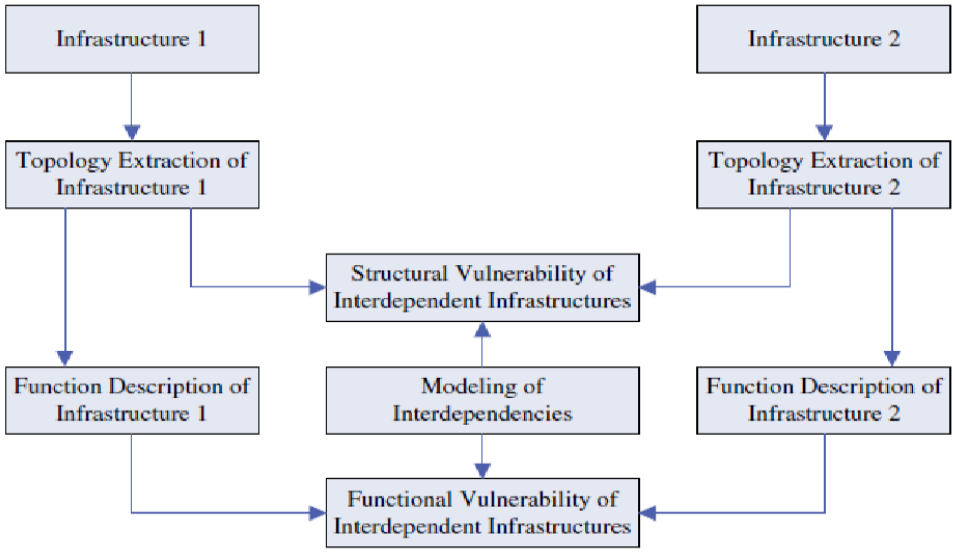


Figure 3. 7: The Vulnerability Analysis Process of Interdependent Infrastructures (Ouyang et al. 2009)

Palmaers (2013) defines vulnerability management as the process of identifying vulnerabilities and evaluating the risks of these vulnerabilities. This evaluation is focussed on correcting the vulnerabilities and removing associated risks.

Qualys (2008) stated the objective of Vulnerability Management is to detect and remediate vulnerabilities in a manner that is timely (Qualys 2008). However, the aspect of timeliness is not adequately defined. This research attempts to address this issue of timeliness by using the example of scheduled scans that Assets such as systems in government may need to undergo. However, it may be worth noting that vulnerabilities may be known but not addressed due to timing or cost reasons.

As with most organisations and even with Government organisation units, scans are carried out on a quarterly, bi-annually or annually basis. The question of what happens to systems

or components that may be at risk of a vulnerability after a scheduled system or component scan has taken place needs to be addressed. This means that any vulnerability that has not been detected after a scheduled scan would have to wait till the next scan before that vulnerability can be detected. This would leave systems or components vulnerable for a long period of time.

3.6.2 Vulnerability Assessment

Profitt (2008) stated that vulnerability assessment can be used against many different types of systems and although vulnerability assessment shares some commonalities with risk assessment they are different. Steele (2008) presents Vulnerability assessment as a vital part of the risk management process while Profitt (2008) summarises the processes involved in vulnerability assessment as: identifying vulnerabilities, the possibilities of reducing those vulnerabilities and improving the capacity to manage future incidents that may occur.

However, Steele (2008) argues that current methods of carrying out vulnerability assessment fail to consider systems in their entirety and consequently are unable to identify vulnerabilities that are complex (i.e. those vulnerabilities that are as a result of configuration settings and unique system environments). To address this issue, the aspect of assessing vulnerabilities of the components of systems is considered.

The fact that ontologies can be used to model domains of interest is useful. Hence, carrying out vulnerability assessments based on the processes provided by Profitt (2008) is one of the goals of this research.

3.7 Chapter Summary

IT Services provide an important means to implement EGov Services and have been discussed in this chapter based on their types. This sets the background for managing IT Services in terms of criticality. They are naturally related to EGov Services because they provide the basis on which EGov Services operate. This chapter has also resolved the nuances that exist between E-Services, EGov Services and IT Services.

Assets have also been introduced in this chapter because of the support role they play to both IT Services and to EGov Services. This chapter has established that assets are important for the running of IT Services and that IT services are used to invoke EGov Services. A

hallmark of discussions in this chapter, however, is seen in the role assets play in E-Government when presented with different security scenarios. Similarly, attention is drawn to the relationships that may exist between assets in terms of dependence and interdependence relations and a summary of interdependencies based on definitions from different researchers is presented with accompanying scenarios. This provides an open perspective for which scenarios revolving around interdependencies and dependencies are developed and modelled in Chapter 7.

The implications of the knowledge gathered in this thesis are summarised in Table 3.4 below. Furthermore, this chapter has further answered RQ1 and RQ2.

Table 3. 4: Summary Points and Implications for Thesis

Summary Point	**Implications for the thesis**
10.	EGov Service delivery relies on the operations of IT Services. Defining the reliance of an EGov Service on an IT Service stratifies both EGov Services and IT Services in levels of criticality
11.	Integrating services into composite ones may be beneficial. However, it is important to manage the risks associated with implementing this.

Chapter 4: Ontologies and Description Logic (DL)

In this chapter, ontologies are discussed to aid the users understanding of the domain of interest. Ontologies are presented as a unifying framework for describing concepts within the domain of interest and the relationships that exist between those concepts. This chapter discusses how EGov Services and the evolution related-challenges can be analysed using ontologies. Having identified the complexities that are present in E-Government which have been discussed in the preceding chapters, the use of ontologies has the potential to overcome these challenges and complexities.

4.1 The Use of the Semantic Web in E-Government

The semantic web involves the use of a new wave of technologies that enable the use of information resident in another system by another system without causing a fundamental change to the systems themselves or to the operational activities of the organisations concerned (Niemann et al. 2005). The use of semantic technologies enables the semantic interoperability that exists between IT systems which may have data structures, vocabularies or formats that are different without bringing about a change to the core systems themselves (Cregan, 2008).

E-Government is known to be one of the early adopters of semantic web technologies which are increasingly playing an active role in the way the E-Government domain is evolving (Klischewski 2003). It makes use of infrastructure that supports the delivery of EGov Services, syntactic web technology for interoperability, online request of EGov Services etc. The Semantic Web unlike the syntactic web gives information precisely defined meaning which allows better cooperation between computers and users (Paunović et al. 2012).

However, the barriers of using semantic web technology in E-Government are many and varied and include the following:

1. Issues associated with the establishment of a semantic framework and the modelling of the domain considering that the information requirements range over every human endeavour (Arango & Prieto-DiazG. 1989).
2. Creating complex queries involves extensive background knowledge on the different domains being modelled along with E-Government
3. Issues involving solving synonyms and ambiguities

4. Lack of orientation towards service transformation and real-time service provision at web frontend (Charalabidis 2015).

Considering the afore-mentioned issues, several authors have discussed what an intelligent E-Government system should be:

1. Integrated even though coming from different kinds of sources into a distributed software system (Zhu et al. 2007).
2. Enable full automation of the computer systems as well as users of the systems
3. Automation of the routine processes which includes analysing users and user queries, retrieving information and integrating search results (Traunmüller & M. Wimmer 2001)
4. Provide intelligence for SRs and SPs as well as in the network
5. Allow network configurations that are dynamic
6. Support the entire lifecycle of Stakeholders and all the business phases involved.

4.2 The Need for an Ontology in Knowledge Representation

At the core of the semantic web technologies are ontologies (Cregan, 2008). This provides conceptual models for interpreting information provided by web pages. In recent years, the development of domain specific ontologies has gained significant interest especially in the aspect of representing knowledge about things and the relationships that exist between these things in the domain of interest. This has involved the provision of formal vocabularies as well as their intended meanings (Horridge et al. 2011).

The study of ontologies is underpinned in the field of Philosophy where research surrounding it is focussed on the study of existence. Similar definitions of the concept of ontology exist but in the field of computer science, it is used to define the existence of theories.

According to W3C, "*an ontology is used to define the terms that describe and represent an area of knowledge*" (W3C 2004a). It is known for its ability to provide a set of representational terms that are coherent, paired with textual and formal definitions that embody a set of representational design choices (Costa et al. 2016). This involves the definition of classes (or concepts), which are general things in the domain of interest,

relationships that may exist among things and properties (or attributes) those things may have.

Although ontologies are closely related to existing data modelling methodologies, they enable descriptions that are more explicit and richer with emphasis on the formulation of logical constraints and the multiplicity of relationships. In comparison to traditional data schemas and models, ontologies have the capability to represent relations that are far more complex which may be directly linked to the data they describe and have formal logical semantics which facilitate the aspect of automated deductive reasoning (Cregan, 2008).

In the context of knowledge sharing Gruber (1993), defined an ontology as "*an explicit specification of a conceptualization*". This conceptualization is an expression of knowledge that helps humans and computer programs share knowledge about the world in terms of entities, the relationships being held by these entities and the constraints that exist between them. That is, a description (such as specification of a program which is formal) of the existence of relationships and concepts for an agent or group of agents is defined as an ontology. For the conceptualisation to be represented in a concrete form, a knowledge representation language is needed, and this is what forms the specification. By conceptualization, it means that an abstract and simplified view of the world is being represented for some purpose.

Ontologies can therefore be viewed as mechanisms for specification (Gruber 1993). They are usually expressed in logic-based languages and the reason for expressing them this way is so that distinctions that are meaningful and accurate can be made among classes, properties and relations (Boyce & Pahl 2007). According to (Uschold et al. 1998), an ontology can take on a variety of forms but one thing noteworthy of ontologies is that they would include a *vocabulary of terms*, and some *specification of their meaning*.

4.3 The Use of Ontologies for Knowledge Building

Ontology is a knowledge representation (KR) system based on Description Logics (DLs) which is an umbrella name for a family of KR formalisms representing knowledge in various domains (Baader et al. 2005). In the narrower sense and with the use of DLs, an ontology is known as the Terminology box commonly referred to as the T-Box. Facts about individuals in the ontology are known as the Assertion box commonly referred to as the A-Box (Rector 2012).

4.3.1 Defining an Ontology with the Use of a Terminology Box

The T-Box is used to define statements of terms that exist within the domain. It allows for specific definitions of vocabulary within a knowledge domain because of the formal specifications ontologies are known to have. It is also used to define concepts and the hierarchy of those concepts (Giacomo & Lenzerini 1996). Statements in the T-Box tend to remain static over time because of the already defined formal specifications. It contains the names of things and the constraints that form them (Patel-Schneider 2004). Examples of knowledge that exists in the T-Box specific to this research include:

Department *is_a* ServiceProvider.

It is possible to include a constraint by naming a class in the form of ServiceProviderReceiver. This statement can be constrained by saying that only SPs can be SRs.

4.3.2 Defining an Ontology with the Use of the Assertion Box

The A-Box contains extensional knowledge about the domain of interest. It contains individual assertions usually referred to as membership assertions (Baader et al. 2003). It contains knowledge about the individuals or instances that exist within a knowledge domain. For example, Department of Health *is _a* Service Provider declares membership in the Service Provider class for the individual Department of Health.

4.3.3 Example of T-Box and A-Box

Figure 4.1 presents an example of T-Box and A-Box

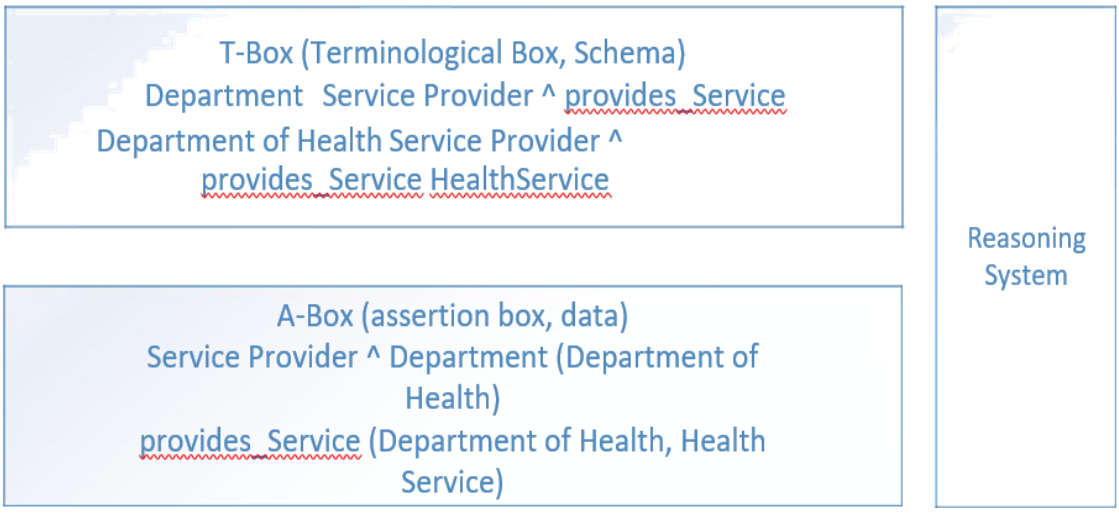


Figure 4. 1: T-Box and A-Box Example

4.4 The Need for the Application of Ontologies in E-Government

The availability of IT solutions to optimise processes in E-Government offers a variety of opportunities for improved data storage, data retrieval and collaboration. However, this may involve mastery of the complexity of E-Government data. The notion of Electronic records management; Semantic Asset management and the development of core vocabularies (Dekkers 2011); issues bordering on interoperability (ISA^2 2017); sharing and reuse of IT solutions (Valayer 2014) are of primary importance to the E-Government domain. Uschold & Jasper (1999) made a differentiation between the different types of ontology-based systems and concluded that ontologies can be used based on the following: *providing common access to information*; *providing an ontology-based specification*; *providing a common ontology/ neutral authoring; carrying out an ontology-based search.* Based on these reasons and applying them to the E-Government domain, this research concludes the following are valid reasons for the use of ontologies in E-Government.

i. **Providing common access to information in E-Government:** Ontologies are used to represent global views especially if information is modelled using different data schemas or cases where data is taken from different sources to make them work as a whole (Ullman 2000). Detailed descriptions concerning the semantics of different data sources are enabled by ontologies which can be used to check ontology consistency.

ii. **Providing an ontology-based specification:** (Bürger et al. 2013; Uschold 2004) pointed out that software specification is an application field for ontologies. Thus, the characterisation and specification of any requirement in a given-domain is made possible with the use of ontologies. The validation and verification of software can be supported by ontologies (Uschold 2004). Also, the formal specification of an ontology allows for changes in the model to be directly propagated during the implementation of the software (Bürger et al. 2013). Thus, software that is consistent with the ontology is developed especially when large software or huge-real time systems in government are being developed. The development of large systems in government may involve high-risk scenarios such as: real-time performance requirements, integration of databases that may be huge and incompatible, external interfaces that keep changing, lack of qualified development personnel etc. An ontology can be used from the initial development of the project to ensure that the project is aligned to the ontology and that significant project failure is avoided.

iii. **Carrying out an ontology-based search:** Ontologies provide the capabilities for searching repositories and supporting navigation and browsing which can encourage structured and comparative searches. Thus, this provides better access to information. However, ontologies have significantly progressed beyond carrying out searches and thus incorporate the aspect of intelligent reasoning which can encourage prediction within the E-Government domain.

4.5 Ontology Languages

Ontologies are accessed using an API and a number of ontology languages are used for their development. Some of these languages include Resource Description Framework (RDF), Web Ontology Language (OWL).

4.5.1 RDF

This language is referred to as a general-purpose language which is used to represent resources on the web (Brickley & Guha 2014). This language is based on the idea that things have properties which also have values and statements can be made to describe their resources (Manola & Miller 2004). It enables the definition of statements about statements and makes use of the concepts of subjects, objects and predicates which are grouped in triples to refer to the different parts that make up a statement (Arroyo & Siorpaes 2014). However,

a major drawback with this language is that it is a very limited ontology language which does not support web services.

4.5.2 Web Ontology Language (OWL) Background

The Web Ontology Language is a family of knowledge representation languages for authoring ontologies (W3C 2009b). It is a semantic web language that represents knowledge which is complex and rich about things, groups of things, and relationships that exist between things. Computer programs can reason based on the knowledge expressed in OWL and can verify the knowledge consistency or make knowledge which is implicit explicit and this is as a result of its logical ability which is computational (W3C 2009b). It is also known as a declarative language that describes things logically with the use of reasoners and can be used to make inferences (W3C 2009b).

The availability of various tools which are used in creating, expressing, editing and reasoning in ontologies make the adoption of OWL in academia and industry highly acceptable (Horridge & Bechhofer 2009). It is an extension of the Resource Description Framework (RDF) which adds vocabularies to existing knowledge structures in tree format (McBride 2004). It provides rules for defining knowledge structures so that based on common structures, instances of knowledge can be created (McGuinness & Harmelen 2004). The semantic web framework can be seen as one that provides a metadata layer in languages that are interoperable in content mainly in RDF of which intelligent or automatic services can be made by machines based on the layer (Li & Wang 2009). The main components of an ontology are classes, individuals and properties (Horridge et al. 2007). A brief description of this is provided thus:

OWL classes: These are also known as sets and are made up of individuals/instances. They may also be referred to as concepts. A class may contain several subclasses and can thus be organised into a superclass-subclass hierarchy which is referred to as a taxonomy. Classes are related to each other because of the existence of subclass relations. Thus, instances in one class are a subset of another and instances are automatically classified as instances of the classes above.

Subclasses can be subsumed by their superclasses and would possess the same characteristics as superclasses. A typical example specific to this ontology is seen in the case where Service Provider is a superclass and is made up of subclasses such as: departments,

Agencies. Thus, all Agencies and Departments are also Service Providers and would inherit the properties of the Service Provider class.

There are also cases where distinct sets of class-subclass hierarchies exist and overlap. Considering that ontologies are not just trees occurring in hierarchies, they are graphs. Therefore, a class can be a subclass of more than one class. There are also cases where there are no instances that are common between classes and this is because the classes can be declared as being disjoint.

Individuals: These are referred to as instances of a class and they represent objects in the domain of interest which have associated properties. A typical example specific to this research is a case where Department which is a class and also a subclass of Service Provider has individuals such as Department 1, Department of Justice, Health Department etc. Individuals can be members of more than one class if it satisfies the classes conditions.

Properties: In OWL, properties are referred to as relationships and three types of relationships exist.

Object Properties**:** these properties link two individuals. Specifying this property involves specifying the Range and Domain of the individuals or classes to be used. Individuals from a specific range can be linked to individuals from another domain. Thus, the specification of range and domains is important in establishing the links and relationships that exist within an ontology.

Data Properties: these types of properties are used to link data type values to individuals.

Annotation Properties: these types of properties are used to add annotations and descriptions to components within the ontology. Although these properties do not add any logical or semantic meaning to the ontology, they can be used to add comments or descriptions to an ontology (Hitzler & Parsia 2009). Figure 4.2 shows the relationships that exist between the ontology constructs.

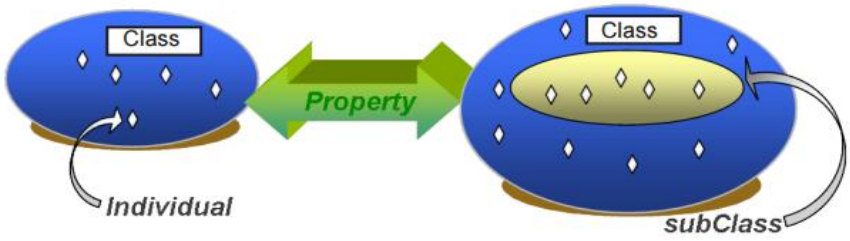


Figure 4. 2: Illustration of Typical Ontology Constructs *(Cregan, 2008)*

Several tools exist for the development of ontologies including the open source tool protégé. However, for developing the ontology, Protégé[80] which is open source and one of the well-known ontology editors has been used.

4.6 Ontology Reasoning

Ontologies can be built and managed more quickly when reasoners are in place because they have the ability to enable sophisticated reasoning techniques and ensure the fidelity of the results gotten after reasoning. The use of the description language OWL-DL allows for the development of a reasoner within an ontology which can be used to make references automatically in the knowledge base (Wang et al., 2006). There are cases where ontologies would need to be reused and the use of reasoners makes it easier for this to happen since reasoners are used to check consistency of ontologies. It is difficult to build ontologies without using reasoners because these ontologies contain the collaborative effort of different experts and have to be integrated into the ontology. According to Wang et al. (2006) "*An OWL ontology is an engineered artefact which may inevitably contain flaws which may include logical inconsistency, unexpected subsumptions and unexpected type coercion for individuals".* Reasoning in ontologies focuses on retrieving information that is not directly modelled or explicitly represented in the ontology and the use of ontologies provide logical semantics to enable reasoning that is automated over data that has been amassed (Cregan, 2008).

[80] https://protege.stanford.edu/

4.7 Methodologies for Creating Ontologies

Developing ontologies requires several processes which also involves identifying the stakeholders (actors) that would be interacting with the ontology. The development of ontologies is divided into two major categories which is also dependent on the setting in which they are applied in:

i. Centralised Ontology Engineering: This type of ontology development methodology involves the ontology development team being in one location. Methodologies that belong to this category include: Methontology (Ferndndez et al. 1997); IDEF5 (Menzel & Mayer 1992); OTK methodology (Semantic Web 2007; Fensel et al. 2001).
ii. Decentralised Ontology Engineering: This is usually used in environments that are large-scale and distributed.

4.7.1 Summary of Ontology Development Methodologies

Based on the discussed ontology development methodologies, this thesis summarises ontology development methodologies may not be fully mature. Thus, a combination of steps or processes in the ontology development methodologies can be adopted. Also, this thesis summarises that the development of an ontology involves the following steps which may not be strictly sequential in order (Ferndndez et al. 1997; Gruninger, M., and Fox 1995; Uschold & King 1995; Bürger et al. 2013).

1. Scoping of the ontology: This may involve identifying the intended users, purpose of the ontology, the competency questions the ontology should answer and user requirements for systems making use of the ontology.
2. Ontology Capture: This may involve the identification of key concepts and relationships within the domain, producing precise definitions for these concepts and relationships, identifying terms to refer to such concepts and relationships.
3. Ontology Encoding: This involves explicit representation of concepts identified during ontology capture phase; the development of a meta ontology to specify the ontology in terms of classes, relationships and entities; the choice of a language that is capable of supporting the meta ontology and the coding of the ontology using the chosen language.

4. Ontology integration: this phase may involve integrating other ontologies with the ontology being developed provided all assumptions within the other ontologies are made explicit. It may also involve identifying synonyms in other ontologies and extending it where no suitable concepts exist.
5. Ontology evaluation: this phase may involve checking for consistency, reusability and clarity of the ontology. Evaluating an ontology may also involve checking the ontology against the purpose for which it was developed as well as checking it against the competency questions.
6. Ontology documentation: documenting the ontology will allow for effective knowledge sharing. It may include documenting assumptions based on the concepts within the ontology.

4.8 A Brief Review of Metadata and Ontologies in E-Government

This section provides an overview of knowledge representation in E-Government and the use of metadata and ontologies that are used to express their semantics. Relevant metadata standards relating to E-Government are presented in relation to the improvements they have made in the E-Government domain.

4.8.1 E-Government Metadata

Metadata is commonly referred to as data about data. It can also be referred to as structured information about a resource (Cabinet Office 2004). They are used in the description of content simply and also in the definition of semantic structures that are complex (Manuel E. Prieto Méndez & Castro 2013). Some identified challenges with the World Wide Web which apply to E-Government can be seen in the areas of encouraging interoperability where data can be shared and exchanged meaningfully and where data originating from different sources can be searched for and retrieved accurately (Ojo & Janowski 2005). The use of the same metadata ensures that the same meaning is shared during the exchange of concepts and that resources are annotated during the specification of the metadata. Semantic gaps occur in cases where different metadata and reference data are used which in turn affects interoperability (Dekkers et al. 2011). Thus, metadata ontologies exist to provide a vocabulary for describing content of information online. An example of a metadata ontology is the Dublin Core.

E-Government databases and repositories are benefitting from the use of metadata in the aspect of managing and finding information (Alasem 2009); the development of digital collections (Tambouris et al. 2007); management of the lifecycle of resources (Haynes 2004). As in other areas of computing, the need to represent content in E-Government has encouraged the incorporation of semantic metadata. Examples of metadata include: contributor, keywords, titles, annotations, descriptions, comments, links etc. These are all applied during the development of the ontology which is shown in Chapter 7.

Several metadata standards exist such as: Dublin Core, Australian Government Locator Services (AGLS), New Zealand Government Locator Services (NZGLS), UK e-Government Metadata Standard (eGMS), Canadian Metadata Standard etc. However, the Dublin Core international standard has been used as the standard by many governments and is an initiative for the description of any digital document. It also provides a set of guidelines for implementing it in text, HTML, XHTML and RDF which encourages interoperability amongst resources (Nilsson & Baker 2008).

4.9 E-Government-Related Ontologies

E-Government-related ontologies offer an infrastructure to cope with heterogenous amounts of information contained in web resources. With the use of metadata that is organised in numerous ontologies that are interrelated Mizoguchi (2004), E-Government related information can be tagged with descriptors that make retrieval, analysis, processing and reconfiguration easy. Information that is related to government is numerous as well as complicated. It has been said that the efficient organization of governments' information would speed up the development of E-Government in any nation (Wen-fei & Xin-li 2008).

4.9.1 Domain Specific E-Government Ontologies

There are several research projects that are involved in the application of semantic web technologies to E-Government.

OntoGov Project

The OntoGov Project developed an ontology that has been built based on the "life event concept" of the national web site of Switzerland (http://www.ch.ch) (Hinkelmann et al. 2010). The OntoGov ontology which is based on Semantic Web services, Business

modelling and SOA principles provides a complex and holistic solution for consistent composition, reconfiguration, and evolution of EGov Services. The OntoGov project as pointed out by (Tambouris et al. 2004) was developed for the testing and validation of an ontology-enabled platform that is semantically-enriched which would constantly facilitate the composition, re-configuration and the development of EGov Services.

The OntoGov ontology is made up of various ontologies which are focused on the description of E-services and their lifecycle. This shows the modular nature in which this ontology was built. This ontology shows certain drawbacks which can be seen in the approach used in building it which was focused mainly on the software engineering side rather than on the detection and orchestration of government services. Also, the interpretation of how the ontologies could be used in practical scenarios is vague. In other words, it is difficult to detect the practicability of its use.

Although the OntoGov ontology was developed with OWL it was seen to lack certain degrees of transparency and expert knowledge for maintenance and usage were required before this ontology could be used. The concept of a Life Event was adopted from the OntoGov ontology during the ontology development phase and was further extended to accommodate Business and Government events. However, the development of this ontology ended in 2006 and the validity of its use in government cannot be traced.

SmartGov Project

This ontology is based on a combination of enterprise and domain ontology and it was built to provide a conceptual description of EGov Services. It provides a conceptual description of EGov Services (Fraser et al. 2003). The SmartGov project was developed as a framework for EGov Services. The aim of the project was to specify, develop, deploy and evaluate a knowledge-based platform to assist public sector employees to generate online transaction services (Macintosh et al. 2003).

The ontology is focused on the social and organisation aspects of EGov Services. The intention of the builders of this ontology was to help public authorities overcome the barriers in planning, designing and delivering electronic services. It consists of a set of relevant top-level concepts that adequately describe service provisioning of the public authority. These concepts include: activities, actors, issues, legislation, needs, process, requirements, responsibilities, results, rights and service types ((Hinkelmann et al. 2010).

This ontology is also focused on increasing efficiency, co-operation and effectiveness by bringing about a common understanding of the principles of EGov Services. What they did in developing the SmartGov ontology was to discover where the "e" was missing in the delivery of government services. The ontology is dominated by terms that have no particular link or association with E-Government.

It is assumed that this ontology is no longer in use today as there are lack of recent publications and evidence. Attempts were also made to contact the developers of this ontology as well as researchers of this ontology, but they were not successful. The concept behind the development of the SmartGov ontology was adopted in our ontology in the area of dominating it with terms which have no particular link to government. This was achieved by incorporating terms relating to Assets, Security etc.

Terregov Project

Terregov makes use of semantic technologies for achieving interoperability and integration between e-government systems. This project involved the development of ontology creation and storage tools to enable the creation of ontologies by domain experts. TerreGov is a European integrated project which involved sixteen partners from eight different countries whose objectives was to enhance the delivery of government services electronically (Bettahar et al. 2005).

This ontology makes use of semantic technologies for achieving interoperability and integration between E-Government systems. This type of ontology did not involve the creation of new ontologies but involved the implementation of tools used to create and store ontologies. This ontology focused on the civil servant and it dealt with interoperability issues of EGov Services for local and regional governments (Sabol et al. 2010). This focus was especially in the delivery of social care services to ordinary citizens (Bettahar et al. 2005). The drawback of this ontology is the absence of focus for a global community. The Terregov European Project proposed a solution to support interoperability between services provided by local government agencies. Furthermore, this project provides centrally controlled orchestrated procedures, involving multiple agencies, to promote transparency and responsibility in E-Government. The Terregov solution is based on social care ontologies specific for the project pilot regions. Finally, multilingualism support is provided by a multilingual reference ontology (D'Atri et al. 2008). However, multilingualism is out of

scope for the ontology to be developed. This study assumes that this ontology is no longer in use today as there is lack of evidence as well as lack of recent publications on this ontology. Attempts were also made to contact the developers of this ontology as well as researchers of this ontology, but all efforts were not successful.

EGov Ontology

The EGov ontology was based on 7 small ontologies which describe varying resources in the E-Government domain. Services that are concrete and abstract are defined in these ontologies. These services include legal documents, organizational units, the flow of information, the decision-making process in the public administration, and all information needed to finalise the configuration of web services (D'Atri et al. 2008). Within the EGOV project, an integrated platform for realizing online one-stop government was developed (Tambouris et al. 2004). It allowed the public sector to provide citizens, business partners and administrative staff with information and public services based on life events and business situations hence increasing the effectiveness, efficiency and quality of public services (Tambouris et al. 2004). Therefore, it was purely aimed at providing information to citizens. The EGov project was very relevant for the OntoGov project. For example, it defined the metadata standard that can be extended into an ontology for the semantic description of the EGov Services. Therefore, it can be seen as the backbone of the OntoGov ontology. Having observed that there is lack of recent publications and lack of evidence of the continuity of the ontology, it is assumed that work on this ontology is discontinued. Attempts were also made to contact the developers of this ontology as well as researchers of this ontology, but all efforts were not successful.

Quonto Ontology

This ontology formalized all the knowledge needed for the realization of a multi-perspective and adaptive evaluation of E-Government portals. It focused on the quality of service that exists within the government. It considered the different perspectives of citizens, experts, technical and the mappings that exist between these different classes of people. With this kind of information, an ontology that enables a comprehensive and holistic view of the quality of EGov Service is created. It consisted of three layers which include 122 concepts, 50 properties and 160 restrictions and it was formalised using OWL which is the standard language for representing ontologies on the web. QUONTO was partially developed using

the open source ontology editor Protégé and was successfully checked for inconsistencies using the Description Logic Reasoner RacerPro. Although the aspect of quality is not included in the TRAO, it provided a basis for developing the ontology based on the different perspectives of major stakeholders. Considering that there have not been recent publications related to this research and attempts to contact the developers of the ontology were not successful, it is assumed that this ontology has been discontinued.

Qualeg ontology

The QUALEG European Project addressed the problem of integrating EGov Services. It proposed the use of ontologies for different purposes: modelling activities performed in the Public Administration; automatically generating a central data repository, the QUALEG database; and managing workflows executed within the QUALEG system. The QUALEG solution is based on 7 ontologies. They include: The Public Administration, including its organizational structure, the processes, the responsibilities and the roles that civil servants can assume in the activities; the data regarding a particular Public Administration; the database schema; the workflows; and the data required by the QUALEG system to execute workflows (D'Atri et al. 2008). This ontology has been discontinued. Also, the practicability of its use in government could not be identified.

QeGS Ontology

160 The QeGS ontology is a three-layer ontology, consisting of 122 concepts, 50 properties and 160 restrictions (Magoutas et al. 2007). This ontology is a multi-perspective evaluation of EGov Service quality (Ouchetto et al. 2012). It is made up of concepts that are high level and relationships between those concepts that describe the meaning of service quality. This ontology offers a reusable platform for the construction of public service systems using an ontological approach (Magoutas et al. 2007). The evolution of services increases the problems associated with the quality of services. This ontology was developed to periodically measure the quality of existing EGov Services as the basis of continuous improvement. Considering that TRAO does not take into consideration the quality of EGov Services, this ontology was not used in the development of TRAO. Furthermore, attempts to contact the developers of this ontology were not successful; it is therefore assumed that this ontology has been discontinued.

4.10 Generic Problems Associated with Existing E-Government Ontologies

Although the goal of E-Government should be the delivery of services to her citizenry, it is unclear in current literature on the possibilities of working jointly to produce these ontologies.

In the area of a joint work force, as stated by (Lamharhar, Chiadmi and Benhlima, 2015; Alazemi, Al-Shehab and Alhakem, 2017; Homburg et al. 2002) there is often a requirement of information exchange in the back offices of government. It is usually difficult to establish a joint workforce because most of the ontologies are developed in isolation and sometimes with no possibility of reuse in mind.

Most concepts or terms are repeated across all ontologies even if they are developed with little or no change in mind. The need for collaborative development is key because the influence of modification of ontologies can be effectively managed (Sunagawa et al. 2003). Although Sunagawa et al. (2003) established the need for collaborative development across E-Government ontologies, it is difficult to conclude that this method of ontology development has been adopted. Within the Netherlands, collaboration is seen between small municipalities. This is aimed at elimination of duplicated efforts and to establish one shared back-office (Janssen & Wagenaar 2004). Since services cannot always be provided at reduced costs and implemented locally; organizations that are small and limited by budgets and expertise cannot develop all the services that are desired. By sharing services and expertise among organizations, a larger number of services can become widely available.

4.11 Chapter Summary

In this chapter, ontologies have been introduced as tools that have a unifying framework for describing concepts within the domain of interest and the relationships that exist between those concepts. With the proliferation of data in the E-Government domain, the use of ontologies would be crucial to the success of enhanced solutions that are integrated. The development of ontologies with the use of semantic technologies provide a basis for its application in real-world scenarios because they have great ability to deliver services that are more intelligent and enable more support for analysing and using knowledge more effectively. OWL is the proposed standard for describing semantics in a machine-accessible way and their used in the creation of ontologies support personalisation of knowledge.

PART III: RESEARCH METHODOLOGY AND FRAMEWORK

Chapter 5: Research Methodologies and Approach

This chapter discusses different methodologies that may be applied in the development of research. The research methodology helps to explain the reasons for conducting a study while considering the different research methods and techniques that are available. The different research methods are discussed briefly to clarify reasons for the adoption of a methodology. There is a focus on the approach adopted for this research and there are further discussions on the research process, the philosophical assumptions on which this research is underpinned based on the aim and objectives outlined in Chapter 1.

5.1 Introduction

Based on the definitions and studies carried out by (Kuhn 1962; Lakatos 1978), generally research can be defined as an activity that contributes to the understanding of a phenomenon. It is also seen as an activity that is well-coordinated which is focussed on adding more knowledge to already existing knowledge (Bryman & Bell 2015).

A methodology as defined by the glossary of information management is *"a system of principles, practices, and procedures applied to a specific branch of knowledge.* It usually refers to the theory of how research should be conducted (Saunders & Rojon 2014). Similarly, the research methodology is linked with the researchers understanding of the research and the strategy employed in answering the research questions (Sue Greener 2008). It encompasses the philosophical assumptions and is not the justification of a choice of data collection methods. It includes the underpinnings upon which a research is based and the implications of the methods that have been used for the research (Saunders 2012).

Methods refer to procedures and techniques by which data which is collected during the research is analysed and the justification for using them. Information about the selected sample, techniques employed in the collection of data as well as the procedures used in the analysis of the data are included in the methods (Saunders et al. 2012).

A phenomenon on its own is typically a set of behaviours of interesting entities (Vaishnavi & Kuechler 2015). This thesis builds on different bodies of knowledge spanning across different research fields. A part of this work focusses on contributions to the Artificial Intelligence (AI) field while some other aspects focus on contribution to the field of Information Systems (IS) research. Considering that the topic of discourse belongs to a set

of overlapping communities and overlapping methodologies, the methodology applied in this research is said to belong to the multi-paradigmatic research community.

5.2 The Research Onion

Sahay (2016) likens the process involved in designing research to address a problem as '*peeling the onion from the centre'.* The reason for this is because he believed that after a problem is identified, researchers begin to work their way through what data, method, techniques or tools are needed to address this problem. The question of whether an onion can be peeled from the centre is one of the reasons for the development of the research onion.

The research onion as proposed by Saunders et al. (2009) shown in Figure 5.1 illustrates how the core of the research onion needs to be considered in relation to other elements of design commonly referred to as the outer layers of the research onion. This is because the researchers understanding and associated decisions in relation to the outer layers of the onion provide the boundaries and context within which data is collected, processed or analysed. Sahay (2016) refers to the outer layers of the onion as the root of the research and the middle layers as the building blocks of research. While the middle layers help to shape the design of the research because they include the strategy employed during the research, the choice of methodology and the time horizon; the outer layers represent the research philosophies and approaches that may be adopted and the preceding layers which involves collection and analysis of data lead to the core layer.

The research follows an adapted version of the research onion because of the different stages that it is made up of and its adaptability to any type of research methodology which can be used in a variety of contexts. It provides a broad perspective as a descriptive model because it can be adapted to different models. The following sections discuss the various stages of the research process while providing reasons for the choices made during the study.

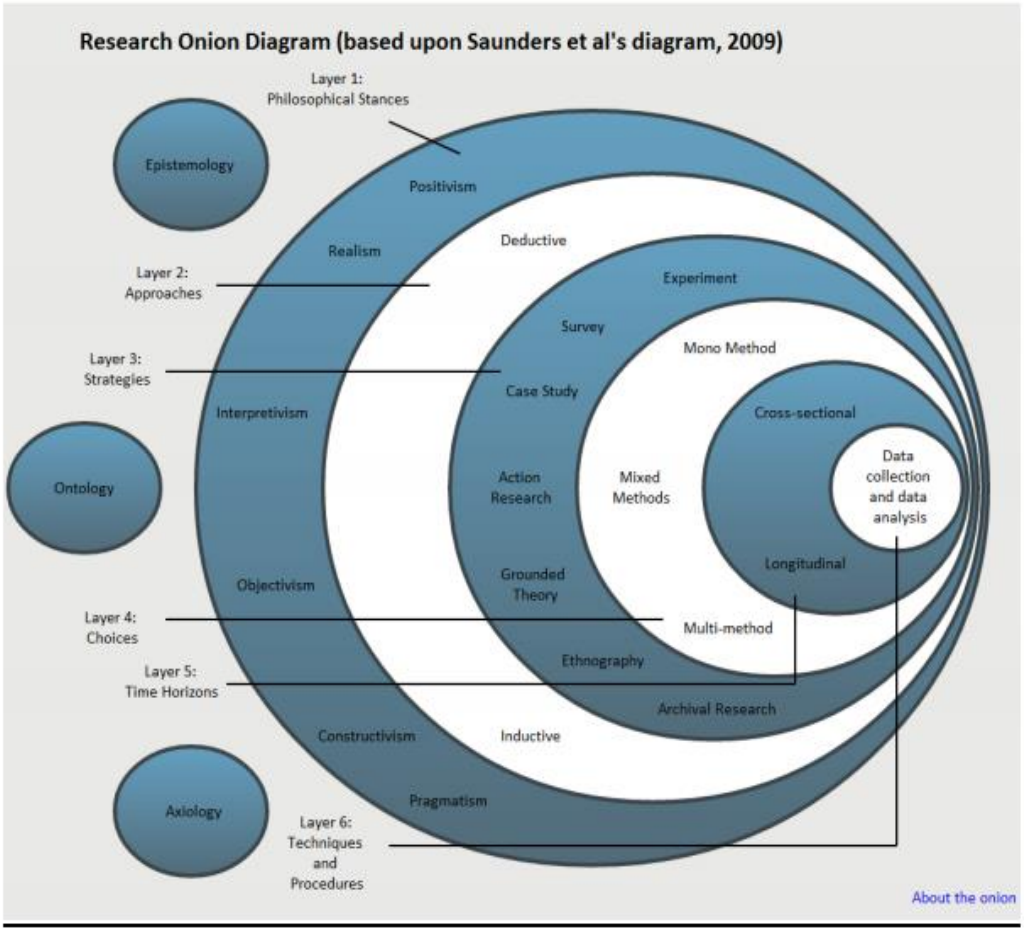


Figure 5. 1: Research Onion showing Assumption Layers based upon Saunders et al's Diagram 2009

5.3 Philosophical Assumptions

The starting point for a research approach that is appropriate is underpinned in the philosophical assumptions. The question guiding the work presented in this study is as follows:

How can governments identify assets or services that are susceptible to risks if these assets or services in governments must evolve and what impacts does this evolution have on services?

The concept of an EGov Service is understood as being linked to social phenomena where there are varying interpretations of its link to specific phenomenon. Studies related to this focus on qualitative aspects of the world which is linked to the Interpretative research philosophy where the focus is usually on the experiences of people, beliefs and attitudes.

In the original Research Onion diagram, the Epistemology, Ontology and Axiology/Methodology assumptions were not included. These aspects tend to exist outside of the Research Onion. However, unlike outer layers of an onion, which are simply discarded as unnecessary; these elements have to be considered explicitly so that a coherent research designed can be explained and justified (Saunders and Tosey, 2012).

Guba & Lincoln (1994) stated that a research paradigm can be shaped by the responses obtained from three fundamental questions which are:

i. The ontological question which asks questions based on what is the form and nature of reality?
ii. The epistemological question i.e. what is the basic belief about knowledge? (i.e. what can be known)
iii. The methodological/axiological question i.e. how can the researcher go about finding out whatever he believes can be known?

However, the choice of research focus is based on the philosophical assumptions assumed based on the relationship that exists between the nature of physical reality(ontology) where questions relating to how the world operates and how this influences this around us have been asked. Furthermore, the research focus has also included the philosophical aspect of epistemology considering that it is concerned with defining knowledge that is acceptable about the field being studied and involves the use of only information that is known to be true which has been subjected to testing that is rigorous (Norris 2005). Clarifying the ontological and epistemological assumptions is important because of the vast number of phenomena a researcher may be subjected to investigate since they help a researcher remain focussed on what knowledge should be obtained. It is also important because it adds to the quality of a researchers work (Patel 2015).

5.3.1 Ontological Assumptions

Crotty (1998) defined an ontology as "the study of being". The ontological assumption is concerned with the nature of the world and human beings in social contexts. It is associated with the central question of whether social entities need to be perceived as subjective or objective (Dudovskiy 2016). Lincoln & Guba (1989) state that the ontological assumptions are those that respond to the question 'what is there that can be known?' or 'what is the nature of reality?'.

This research partly adopts the ontological assumption. The reason for this is because it has been established in preceding chapters that the nature of the research assumes the existence of a world of cause and effect. It is assumed that there are some realities associated with the role that technology plays in the evolution of EGov Services which may eventually pose a risk to government. Thus, this research partly follows a realistic ontology which can be likened to a causal reality. According to Pring (2004), *"One purpose of research is to explain what the cause is or what has happened. A reason for seeking explanations might be to predict what will happen in the future or what would happen if there were to be certain interventions".* This is clearly shown in the research aim of the study that is targeted at analysing the effects of evolution in terms of risks, threats and vulnerabilities of EGov Services on the assets that are involved. Thus, this research is concerned with looking at what will happen to EGov Services and the assets they make use of while evolution occurs. It is assumed that the effect in terms of risks is attributed to the different types of evolution occurring at different levels.

5.3.2 Epistemological Assumptions

Epistemology *is 'a way of understanding and explaining how we know what we know'* (Crotty 1998). Based on the Research Onion, the epistemological assumption is divided into four different types which are positivism, realism, pragmatism and interpretivism. It is also concerned with the provision of a philosophical grounding for making decisions on what kinds of knowledge are possible and how a researcher can ensure that the knowledge gotten is both legitimate and adequate (Crotty 1998).

Positivist Research Paradigm

The positivist research paradigm believes in the possibility to observe and describe reality from an objective viewpoint. It generates testable hypotheses (or research questions) that allow explanations which are measured against accepted knowledge of the world we live in. It creates a body of research which will generate the same results if replicated by other researchers (Sue Greener 2008). This research paradigm assumes that reality exists independent of the subject being studied.

Realism Research Paradigm

This is similar to positivism in its beliefs and processes because it believes that the researcher and social reality are independent of each other and so the possibility of creating results that are biased are limited (Saunders et al. 2012). However, realism differs from positivism because it believes that all theory can be revised because scientific methods are not perfect. It also believes that knowing what if further research is not carried out and if researchers don't open up their minds to new methods of research, then reality may not exist.

Pragmatic Research Paradigm

This research paradigm can yield better insights given that it has the potential to allow for the mixing of methods. Pansiri (2006) posit that researchers have the freedom of choice to select methods that best suit their needs. The research methods used under pragmatism are decided based on the kind of questions asked. Since it is driven by consequences, it is important that the right kind of questions are asked. Another feature of this research paradigm is that it is used for research that occur in the political, historical or social contexts which is relevant for this research.

Interpretive Research Paradigm

Interpretive research focuses on understanding phenomena through the meanings that *people* assign to them (Orlikowski & Baroudi 1991). It assumes that access to reality is *"through social constructions such as language, consciousness, shared meanings, and instruments"* (Myers 2009). This method of research is usually based on a near-experience or historical perspective. Thus, the basic generation of meaning is always social. This is because the researcher doesn't start with concepts previously determined but allows this emerge from encounters in the field. Encounters in the field could encompass areas related to fieldwork or textual-archival research. Both aspects have been extensively used during this research.

5.3.3 Justification of Philosophical Choice and Rationale

The interpretive research paradigm is adequate for carrying out investigations on EGov Services and the SPs responsible for their management. This is because the E-Government domain is a complex one and there is little unanimity in literature regarding definitions of key concepts and ways on how to investigate ownership of them in ways that are consistent or systematic. Understanding how EGov Services are composed in relation to the risks their composition may face as evolution occurs is based on my interpretation which can be

generally linked to the interpretative research approach. This assumption is visible in the research question presented because this question is initiated with the modal verb *can*, and not *should*. This shows that the investigation carried out is done without the use of normative aims for illustrating or testing how it should be done. Therefore, the aim of this thesis is to provide a useful way of investigating evolution-related risks in relation to EGov Services. However, this thesis does not claim to provide the only way of investigating these types of risks.

5.3.4 The Use of Hermeneutic Analysis for the Interpretive Paradigm

The formulation of the conceptual framework is based on conducting the literature review as a hermeneutic process. The hermeneutic process can also be referred to as a qualitative research strategy. Hermeneutics is derived from the Greek word ermhneuein (hermeneuin), meaning to interpret and its derivative (hermeneia) meaning interpretation. It was developed in the context of interpreting biblical texts and was later extended to the interpretation of all textual material and furthermore extended to the subject of general understanding (Ramberg & Gjesdal 2005). Sequel to understanding in general, the paradigm of modern hermeneutics is thoroughly explained in *Wahrheit und Methode* (1960) by Hans-Georg Gadamer (Gadamer 1965). This analysis involves different methods of analysis which are based on carrying out interpretations. These interpretations allow one to gain an in-depth understanding of the research phenomenon being discussed.

The hermeneutic analysis is tightly related to the Interpretive research paradigm which strongly asserts that interpreting meanings results in understanding (Myers 2009; Butler 1998; Klein & Myers 1999). It is different from other research strategies which focus on independence of interpretations that are subjective and objective in the formation of knowledge. It involves the use of different approaches providing a platform to carry out in-depth understanding of meanings which require interpretations that are systematic.

To adequately interpret and understand meanings, this research method allows its combination with other methods of analysis. It involves identifying concepts and different terms used to describe it. The researchers understanding is broadened based on reading publications and refining further publications during this process. The process of reviewing and analysing processes is intertwined and iterative which are focussed on identifying themes that are interesting or contrasts and gaps in the body of literature. This approach has

fostered the continuous review of literature, E-Government policy documents and practices with the intention to understand the evolving nature of EGov Services.

Contemporary hermeneutics can be divided into four distinct perspectives which are conservative, constructivist (pragmatic) critical, radical (deconstructionist). Table 5.1 presents a summary of the hermeneutic perspectives presented by (Coyne 1995).

Table 5. 1: Hermeneutic Perspectives (adapted from Coyne, 1995)

Perspective	Main theme	Proponents
Conservative	The task is to uncover the original meanings of the action-text as intended by the author. Objective, a-historical, and a-contextual purposeful meanings are secured from the correct and decidable interpretation.	Emilio Betti (1955) and Eric Hirsch (1967), to name but two.
Pragmatic (Constructivist)	Interpretation here involves entering into the interpretative norms of a community; meaning here operates and is to be found within the historical contexts of the interpreter and interpreted.	Hans Georg Gadamer (1975), Ludwig Wittgenstein (1953)
Critical	The purpose of interpretation here is emancipatory; conventional wisdoms within communities are challenged in order to address potential power asymmetries	Karl-Otto Apel (1980) and Jurgen Habermas (1972, 1980).
Radical (Deconstructionist)	Here texts and social action are treated as an endless play of signs that reveal and conceal knowledge through the play of difference and contradiction.	Jacques Derrida (1970, 1976).

Constructivist Research Method

This research method involves constructing knowledge by people actively involved in the research process. It accepts reality as a construct of the human mind and thus perceives reality to be subjective (Dudovskiy 2016). It also recognises that research is a product of the values of researchers and cannot work independent of them (Schwandt 2000). With this method, the researcher relies mostly on qualitative data collection methods and analysis of both the qualitative and quantitative (mixed) methods. In the words of David Elkind *"Constructivism is the recognition that reality is a product of human intelligence interacting with experience in the real world. As soon as you include human mental activity in the process of knowing reality, you have accepted constructivism"* (David Elkind 2004). The constructivist research method provides a basis for understanding the nature of what is being studied (ontological assumption) and also provides a basis for understanding how research can be undertaken by the researcher to make knowledge claims (epistemological assumption).

Critical Research Method

This research method is used to challenge conventional conceptual and theoretical knowledge bases and methods. It asks questions that go beyond prevailing assumptions and understandings and assumes the role of power (Jupp 2006). This method was not employed in the research as the research was not focussed on challenging the powers that be or confronting conventional practices in the E-Gov domain.

5.3.5 Choice of Method and Rationale

Based on the recommendations of (Klein & Myers 1999; Butler 1998), this research makes the argument that the constructivism hermeneutic research method is a needed E-Government reform that will succeed when the aspects of assets, risks, stakeholders and EGov Services are properly aligned. There is the need for an integrated social constructivist approach towards the study of the application of technology in E-Government.

Based on every possible interpretation, constructivism will only fail in this research if the aspects of assets, risks, stakeholders and EGov Services are not properly aligned with technology. Although the argument that the use of technology in E-Government may have sufficient impetus to encourage the alignment of aspects of assets, risks, stakeholders and EGov Services, the true success of reform in the E-Government domain with respect to evolution will be truly rewarding if the constructivist method is incorporated.

5.4 Research Design Choice

The choice of research design method is based on the third layer of the research onion. This layer is essential in designing the research. Vaus (2001) argues that *"the function of a research design is to ensure that the evidence obtained enables a researcher answer the initial question as unambiguously as possible"*. It focuses on the aspect of designing the research based on varying methods which can be quantitative, qualitative or a mixture of both. Saunders et al. (2012) outlines six different methodology choices which are: mono method quantitative, mono method qualitative, multimethod quantitative, multimethod qualitative, mixed method simple, mixed method complex. While choosing a methodology, a corresponding analysis procedure can be applied. However, most researchers are conversant with the qualitative and quantitative research methods. The other methods

described by Saunders et al. (2012) are derivatives of the qualitative and quantitative methods.

5.4.1 Qualitative Research Design Method

This is usually used in exploratory research to gain understanding of opinions, uncover trends, get motivations and underlying reasons about a problem (DeFranzo 2011). They tend to interpret and make sense of phenomena based on meanings people assign to them because studies are based on natural setting (Greenhalgh & Taylor 1997; Denkin 1994). According to Denkin (1994), researchers who use qualitative methods seek a deeper truth and make use of a holistic perspective which preserves the complexities associated with human behaviour. It doesn't involve the use of numbers or numerical data. The qualitative method of data collection is focussed on the collection of data usually from a smaller sample which is why it may be referred to as an expensive research method. Respondents are carefully selected to fulfil a certain quota. The reason for this is because the data collection methods are time-consuming. The qualitative research method is known for its ability to provide insights into problems and to help develop hypotheses for potential quantitative research (DeFranzo 2011; Greenhalgh & Taylor 1997). It also gives an in-depth picture on how and why things have happened. The use of the qualitative method can enhance the development of quality measures as well as the quality improvement of efforts (Sofaer 2002). The techniques used by researchers for collecting quantitative data can be classified in terms of unstructured or semi-structured techniques. These include: focus groups (group discussions), action research, observations/participation, individual interviews, case studies, pictures, photographs, cognitive interviews.

Monomethod Qualitative

This involves the use of a single qualitative data collection technique and corresponding analysis procedure. Data collection techniques may involve the use of only questionnaires or observations etc (Saunders & Tosey 2013). The monomethod research design method is restrictive considering the complexity of the research. Thus, this method was not employed.

Multimethod Qualitative Design

This involves the use of more than one data collection technique. It may involve the use of in-depth interviews and diary accounts with associated analysis procedures (Saunders &

Tosey 2013). Considering the complexity of the research topic, it was impossible to use only one research design method. Thus, the multimethod qualitative design method was not used.

5.4.2 Quantitative Research Design Method

This method quantifies a problem by generating numerical data or data that can be transformed into statistics that is classified as usable (DeFranzo 2011). The data produced with the use of the quantitative method are always numerical and are analysed with the use of statistical and mathematical methods. It is a research method that involves the use of numbers. Attitudes, opinions, behaviours, are usually quantified using this method which are usually generalised results from a larger sample size. Facts are formulated and patterns are uncovered with the use of measurable data. The data collection techniques in the quantitative method are usually structured as opposed to the Qualitative data collection method. Techniques used in this method include: surveys, telephone interviews, face-to-face-interviews, website interceptors, online poles, longitudinal studies, systematic observations, secondary data.

Monomethod Quantitative

This involves the use of a single quantitative data collection technique and corresponding analysis procedure. Data collection techniques may involve the use of only in-depth interviews etc. Since data was not being quantified in this research, it was not possible to use this research design method.

Multimethod Quantitative Design

This involves the use of more than one quantitative data collection technique. It may involve the use of a combination of techniques like questionnaires, structured observations etc. More than one quantitative data collection technique is used in this method (Saunders & Tosey 2013). Restriction to only this research design method would not have produced the right results considering that using this method alone would have proved weak in understanding the setting and context for data collection.

5.4.3 Mixed Methods Research Design

The mixed methods research focusses on the adoption of a strategy that makes use of more than one type of research method. This could be a mix of qualitative and quantitative

methods, a mix of just qualitative methods or a mix of just quantitative methods (Brannen 2005; Byrne & Humble 2007; Saunders & Tosey 2013). This method of research is also referred to as the multi-strategy research method (Bryman 2001). Mingers (2003) suggests that researchers do not have to restrict themselves to a single research method and thus can combine the qualitative or quantitative research methods. This concept of combination is referred to as triangulation. It incorporates the use of multiple approaches at all levels of the research (Byrne & Humble 2007). This research method could start with a particular data collection technique or analysis procedure and the method of data collection can change in the course of the study (Saunders & Tosey 2013).

5.4.4 Rationale for Research Design Choice

Considering that the mixed methods focusses on the use of a combination of more than one type of research method, it was adopted in this research. This choice was made because this method provides multiple ways to explore the research problem. This method enables the researcher to develop a better understanding of our social world especially in the context of E-Government. This potentially provides ways to uncover patterns that are unexpected and generates new avenues for research while refining the researcher's knowledge of social processes. The complexity of data to be gathered for this study made it difficult to use a single method in isolation. Thus, a combination of methods had to be adopted.

5.5 Research Strategy and Data Collection Methods

The fourth layer of the research onion presents the different research strategies that can be applied when conducting a research. However, only the prominent ones will be examined in this research.

There are four main data collection techniques presented: 1) in-depth interviews 2) the use of a case study 3) IT artefacts 4) archival research. In addition to these research techniques, documents were also used. The use of focus groups was not applied during the research given that the research being conducted is socially sensitive; Observations weren't used because this level of access into government was not possible. The techniques used in data collection are discussed based on their applicability especially in relation to the scenarios generated from the case study in Chapter 7.

Interview

Interviews are usually used for qualitative research and especially in interpretive case studies. It involves face to face conversation with the purpose of exploring issues or topics in detail. In this research strategy, pre-set questions are not defined but this is shaped by a defined set of topics. They can be used to explore the experiences, beliefs, views and motivations of individual participants (Gill et al. 2008). Interviews could either be structured, semi-structured or unstructured. They are usually used when there is little already known about the phenomena being studied.

Most of the interviews conducted during this research were conducted remotely using Electronic video means (Skype), phone calls so that participation could be enabled and encouraged. Weller (2015) posits that the use of remote interviews has the potential to widen the participation of interviewees considering the constraints of time and space are compressed.

The initial interviews involved the use of questions that were less structured which was used to stimulate the interviewees thoughts in the research area. This was done to evaluate their understanding of the current processes and IT artefacts in use and their expectations of future processes and the construction of emerging IT artefacts. The completion of the initial interview stages set the ground for rigorous studying and observations so that more knowledge could be gained on the subject and in-depth interviews could be conducted.

In-depth Interview

The initial interview method set the background for conducting in-depth interviews. Most of these interviews were conducted by electronic means (Skype). This research technique is used to get a vivid picture of the interviewees perspective on the topic being researched. This involves interviewing a person who is considered the expert and the interviewer assuming the role of student (Mack et al. 2005). The reason the interviewer/researcher assumes the role of student is so that he/she can learn everything the interviewee has to share about the topic being researched. This involves posing questions in manners that are neutral and listening to the responses to these questions attentively. This research technique does not encourage leading participants to any preconceived notions nor do they encourage the provision of answers by gestures of approval or disapproval. This research technique keeps gaining increasing popularity because of its effectiveness in giving a human face to research

problems (Mack et al. 2005). The strengths of this method can be seen in its elicitation of in-depth responses with contradictions and nuances; the establishment of connections and relationships seen between particular phenomena, events and beliefs.

Case Study

The usefulness of case studies is seen when a research question seeks to explain some present circumstance (Yin 2009). Case studies are used to provide better understanding on issues that are complex and can be used to add experience to what is already known through research that was conducted previously. They are also used to extend experience in a particular field (Soy 1997). Case studies can take on a number of forms which could be in the form of describing an event, exploratory or explanatory (Sauro 2015). The focus of a case study is usually an organisation, entity, individual or event. Data collection is usually with the use of observation, documents, interviews or reports. The case study frequently draws upon a mixture of methods.

The use of a case study was employed in this research and this involved developing an interpretive case study based on a given set of scenarios in Chapter 7. The design of the interpretive case study involved the study of literature on the developments of IT within government in the UK and also establishing relationships with major stakeholders (SPs) in the UK Government. The relationships with the SPs involved carrying out in-depth interviews on the current operations within government and analysis of the current risk mitigation plan with respect to evolution. Although this was a long process, it enabled the researcher develop scenarios that can be applied to real world government systems.

Artefacts

(Goetz & LeCompte 1984) defined artefacts of interest to researchers as things that people make and use. Analysing artefacts can also be seen as a process through which users of the artefact and the culture in which it exists are understood. The use of artefacts provides an opportunity for the design researcher to generate inspiration and insights for future product/service designs. Collecting and analysing texts and artefacts can greatly foster understanding of the phenomenon being studied (RWJF 2008). Artefacts are constructed within a given context and it is necessary to consider the various aspects of an artefact. It is also important to establish the uses of an artefact as well as the unintended uses. Doing this may possibly open up additional avenues for other areas of research. In developing an

artefact, it may be necessary to draw up a questionnaire on the types of things the artefact should be involved in doing.

(Goetz & LeCompte 1984) identified four activities involved in identifying artefacts which are: locating the artefact, identifying materials, analysing it and evaluating it. Their recommendation is based on the fact that the more informed a researcher is about a setting or subject; the more useful artefacts are identified and the more easily access may be gained to those artefacts.

Artefacts were employed in the course of this research because of their importance in providing information about the operations in E-Government. It was useful in the development of the ontology and corresponding tool since the studied artefacts revealed current lapses and enabled meanings to be assigned in the course of the research. Sources of the artefacts used in this research were gotten from valid sources such as books, peer-reviewed journals and conference papers, E-Government websites such as the Gov.uk, UK national archives.

Phenomenological

This is a qualitative strategy that involves the use of a combination of methods such as reading documents, conducting interviews, visiting places etc. to understand the meaning that is placed on what is being examined (Sauro 2015). The focus is usually on people who have experienced a phenomenon and data collection is usually carried out by interviews. The sample size is usually between 5 to 25. It involves gathering deep information and perceptions about a phenomenon. Considering that the approaches involve a collection of subjectivity and personal knowledge, it was important in analysing key stakeholders' personal perspectives and interpretation related to the existing artefact. This strategy was useful during the research considering that the research was not limited to only one research strategy.

Grounded Theory

This strategy is relevant to this research considering that it is focussed on providing a theory or explanation behind an event. Strauss & Corbin (1994) opined that it is "*a general methodology for the development of theory that is grounded in data that is systematically gathered and analysed".* It involves the use of existing documents and interviews to build a

theory based on the data obtained. It leads the researcher to begin the study without notions that are preconceived on what the research question should be about but rather assumes that the theory on which the study is based will be tested and refined during the research (AECT 2001). The sample sizes are usually larger and are used to establish a theory (Sauro 2015). The focus is usually on the development of a theory from grounded data. Data collection involves the use of interviews and open axial coding. The sample size is usually between 20 to 60. The purpose of using this methodology is to develop theory through data and theoretical analysis processes that are iterative while verifying the hypotheses throughout the study (AECT 2001).

5.5.1 Rationale for the Research Strategy and Data Collection Method

Considering that the mixed method research design choice was employed during the design stage of the research; several methods of collecting data had to be used. The achievement of the aims of the research were subject to the collection of substantial data through appropriate methods of research. The use of interviews, case study, artefacts and archival research were used during the data collection phase. The choice of interviews and a further engagement in in-depth interviews allowed for the refinement of data as well as the modification of scenarios to suit the case study. Furthermore, the choice of the phenomenological strategy was employed given that stakeholders were able to share their personal perspectives on the subject area. Also, open and axial coding from the grounded research method were used because relationships had to be established based on meanings that emerged from the data collected. These were useful in the development of the ontology.

5.6 Justification of the Need for an IT Artefact in the Research

This section justifies the need for an IT artefact in this research. Usually once an IT artefact is built, the IT artefact tends to be taken for granted, presumed to be unproblematic or even disappears from the view (Orlikowski & Iacono 2001). The reason this is discussed is so that technology can be taken seriously in terms of its ability to enhance operations and processes given the research context but not without preparation for its associated consequences. Table 5.2 provides definitions of IT artefacts that have been adapted for this research.

Table 5. 2: Definition of IT Artefact

S/No	Definition	Source
1.	"an entity/object, or a bundle thereof, intentionally engineered to benefit certain people with certain purposes and goals in certain contexts. It is developed, introduced, adopted, operated, modified, adapted, discarded, and researched within contexts and with various perspectives" (p. 121).	Zhang et al. (2011)
2.	"the integration of the processing logic found in computers with the massive stores of databases and the connectivity of communication networks", so that it "includes IT infrastructure, innovations with technology, and especially the Internet" (p. 394)	Agarwal et al. (2005)
3.	"constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), and instantiations (implemented and prototype systems)" (p. 77)	(Hevner *et al.*, 2004)
4.	"systematic processing of information in human enterprise" (p. 541)	King & Lyytinen (2004)
5.	"the application of IT to enable or support some task(s) embedded within a structure(s) that itself is embedded within a context(s)," whereby its hardware/software design "encapsulates the structures, routines, norms, and values implicit in the rich contexts within which the artefact is embedded" (p. 186)	Benbasat & Zmud (2003)
6.	"bundles of material and cultural properties packaged in some socially recognizable form such as hardware and/or software" (p. 121)	Orlikowski & Iacono (2001)

An IT artefact is something that is made and has information technology as a component. This research is interested in providing an understanding of what IT artefacts are in the

context of the study and how IT artefacts are approached during the study. Based on the definitions of an IT artefact in table 5.2, the study adopts the following: (1) they are dynamic and can be developed, adopted, modified (2) they are not natural, universal, given or neutral, (3) they are neither fixed nor independent but emerge from economic and social practices, (4) they are integratable, (5) they are always embedded in some time, community, discourse or place. (6) they exist in the form of hardware or software, (7) they include IT infrastructure.

The view on the presence of technology in this thesis corresponds with what Orlikowski & Iacono (2001) call an ensemble view of technology in which technology is often studied in terms of (1) how it can be used in certain ways and (2) how technology comes to be developed. Furthermore, Zhang et al. (2011) discuss technology in terms of (1) its constantly evolving and transforming nature which is capable of transforming and forming new phenomena and (2) the challenges associated with the evolving use of technology in different contexts. This thesis is concerned with the discussion put forward by Zhang et al. (2011).

5.7 Research Method

Based on the constructivist research method which was adopted as the research method, the theory suggests that risks are only socially processed if they are cognitively constructed by social agents (Figueiredo et al. 2014). Thus, making many problems invisible. Furthermore, this thesis takes a fundamental part of its bearing in intelligence analysis which is increasingly being driven by the need for intelligence in ways that are unpredictable which require special expertise and the performance of core intelligence functions (Lillbacka 2013).

Systems in government must evolve while responding to a myriad of changes in government. Therefore, the E-Government system must be designed to cope with a number of security issues associated with evolving systems or components. The issue of making theoretical assumptions on which the design of a system is based should be avoided. Garlan et al. (1995) posits that architectural mismatches are a major universal source of problems and are a direct result of assumptions that are mismatched. Another cause for failures in systems which is a risk is when invalid assumptions about operations in the real world are made by designers (Lipson 2006).

Thus, this thesis takes the stance of Lipson (2006) in designing the system for analysing evolution-related risks. It posits that:

"in the absence of countermeasures, a system's security and survivability will degrade over time. Changes in the environment or usage of a system, or changes to the elements that compose the system, often introduce new or elevated threats that the system was not designed to handle and is ill-prepared to defend itself against. The first step in evolving to meet new threats to your system's security and survivability is to recognize the need to modify your system — that is, to recognize changes in security and survivability risks that trigger the need to enter the evolution phase of the system development life cycle".

It is therefore essential to devote significant risk management resources to the ongoing evolution of any mission critical system. Again, this highlights the importance of intelligence analysis which the use of an ontology will provide. An ontology has predictive and detective capabilities given that it may be able to detect the changes that may affect assets. The assumptions made by an ontology through the inference engine will help in detecting changes that may affect assets on which the security of the system is founded.

The work presented in this thesis is the result of the use of five interrelated research activities; i. the extensive review of relevant literature relating to the subject area (Chapters 2,3 and 4) ii. the formulation of a conceptual framework (Chapter 6) iii. The use of an interpretive case study (Chapter 7) and iv. The creation of meaningful artefacts with the use of a tool (Chapter 7 and 8).

5.7.1 Systematic Review of Relevant Literature

A systematic review of literature was carried out. This was based on the hermeneutic process and it was done to identify gaps in existing knowledge. Organised searches were conducted which resulted in a vast amount of scholarly work. This involved searching databases, electronic documents, books, library catalogues, journals, policy documents, E-Government materials, websites, blogs, social media posts etc. using pre-defined keywords and synthesizing key ideas, theories and concepts of this search into a conceptual framework. Carrying out the literature review involved making interpretations of other research studies which provided more depth on areas to be included within the development of the literature. Searches were carried out using a combination of keywords to capture as many research materials as possible. Generalisations were avoided and the researcher tried to narrow searches by being specific.

The hermeneutic method makes use of alternative perspectives where an object is examined from different angles with each examination improving the understanding of the object. Pentti (2007) described this alternation of viewing points as the hermeneutic circle or the hermeneutic spiral. This implies that steps are repeated and are used to get a deeper understanding of the problem. Thus, it can be said that all understanding or new knowledge is based on previous understanding or old knowledge. This cycle doesn't end until no more interesting findings are discovered. Fundamentally, reviewing literature is a hermeneutic process which can be better described if references are made to the hermeneutic circle (Boell & Cezec-Kecmanovic 2011).

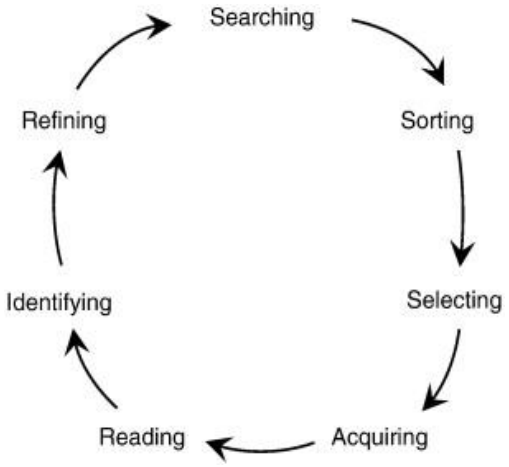


Figure 5. 2: The Hermeneutic Circle for Undertaking Literature Reviews (adapted from Boell & Cezec-Kecmanovic, 2011, p.9)

The literature review helped in identifying where previous researchers had reached in the study and where the researcher can build upon based on previous studies. It included dividing areas of discourse into thematic headings and researching on those areas. Each literature search was linked to the challenges and contributions surrounding the central theme of the research.

The literature review on E-Government and surrounding topics is vast with different researchers providing insights based on their perspectives. However, this served as the focal point of the literature review with areas such as: evolution of assets, evolution of EGov Services, risks associated with evolution etc. so that the theoretical discussion on evolution in E-Government was accommodated. This produced a trail of related articles in this field with some of the articles building on the works of others.

These searches were focussed on retrieving accurate, reliable and up-to-date material which has prepared the ground for the application of these new ideas to new areas of research. The literature search was extensively carried out in the areas of evolution in E-Government as this form the focal point of search for the study. Carrying out this search provided a good range of material which were developed based on different researchers' perspectives. Some of the materials were skimmed through to get cues for the research and in the event that they were not particularly suited to the research focus, more materials were added to the search. The literature review does not claim to be all inclusive or complete but it can be said that it has added cumulative meaning to the growing body of existing knowledge.

5.7.2 Formulation of a Conceptual Framework

Jabareen (2009) defines conceptual frameworks as *"products of qualitative processes of theorization"*. The formulation of the conceptual framework is based on conducting the literature review as a hermeneutic process. The hermeneutic process can also be referred to as a qualitative research strategy. The conceptual framework is a key part of the research design and it includes assumptions, system of concepts, beliefs, expectations and theories that support and inform the research (Miles & Huberman 1994). Developing a conceptual framework is important because it enables a researcher to show the relationship between the different constructs that he intends to investigate. It also presents a preferred approach that can be used in defining an idea. It also brings focus to the research and acts as a link between the literature review, methodology and intended results (Datt 2015).

The development of the conceptual framework for this research was based on the identification of important concepts for the research and logically linking them together. The focus while linking concepts together was on determining the relationships and inter-relationships between them. The conceptual framework is presented in chapter 6. However, the development of the conceptual framework involved the generation of research questions which were refined throughout the research period.

5.7.3 The Design of an Interpretive Case Study

The design of an interpretive case study involved the study of literature on the developments of IT within government in the UK and also establishing relationships with major stakeholders (Service Providers) in the UK Government. Some of the relationships were fostered and led to the development of the case study while some were never well received.

The relationships with the Service Providers involved carrying out in-depth interviews on the current operations within government and analysis of the current risk mitigation plan with respect to evolution. The results of the written case study are shown in Chapter 9. Although this was a long process, it enabled the researcher develop scenarios that can be applied to real world government systems.

5.7.4 The Use of the Design Science Research (DSR) Methodology in Creating Research Artefact

DSR is derived from the engineering discipline and it is concerned with the science of the artificial (March & Smith 1995). The creation of artefacts that are meaningful which have the ability to change already-existent situations to preferred ones remains the focus of the Design Science Research Methodology (Simon 1996). It is used in the development of new solutions to existing but unsolved problems and matching solutions to problems that may be new or unsolved (Holmström et al. 2009). It is gaining growing attention in literatures related to information systems (Fischer et al. 2010). It involves the creation of new knowledge through the design of novel or innovative artefacts to improve and understand aspects of Information Systems (Vaishnavi & Kuechler 2015). DSR is mostly considered a problem-solving paradigm rather than a problem understanding paradigm and this is because it embodies prescriptive knowledge in IT artefacts that are used in solving business problems (Hevner *et al.*, 2004).

The DSR approach is used in building the IT artefact in this study because it is important to consider the relevance of the IT artefact for the already set out requirements so that a solution can be arrived at. According to McKay & Marshall (2005), it can be seen as another research approach to solve relevant problems practically. The focus while developing the IT artefact is on the problem itself. Understanding why an IT artefact works or does not work is necessary to the creation of the IT artefact (Hevner *et al.*, 2004). Also, the underlying kernel theories of an IT artefact have to be understood so that the reason for the creation of an IT artefact are clear to the reader. These theories are created by the experience and creativity of the researcher and are defined by the modification of social science and natural theories (Hevner et al. 2004; Markus & Robey 1988). These theories have been presented in sections 5.3.6 and 5.7.

The creation of DSR methodology by (Peffers et al. 2008) was based on three objectives: "(1) provision of a nominal process for conducting DS research, (2) building upon prior literature about DS in IS and reference disciplines, and (3) providing researchers with a mental model or template for a structure for research outputs." The DSR methodology includes six steps which involve the following: identification of the problem, definition of a solution laid out by clear objectives, design and development, demonstration, evaluation and communication. This is presented in figure 5.3 and a description of the steps including the activities involved is presented in table 5.3.

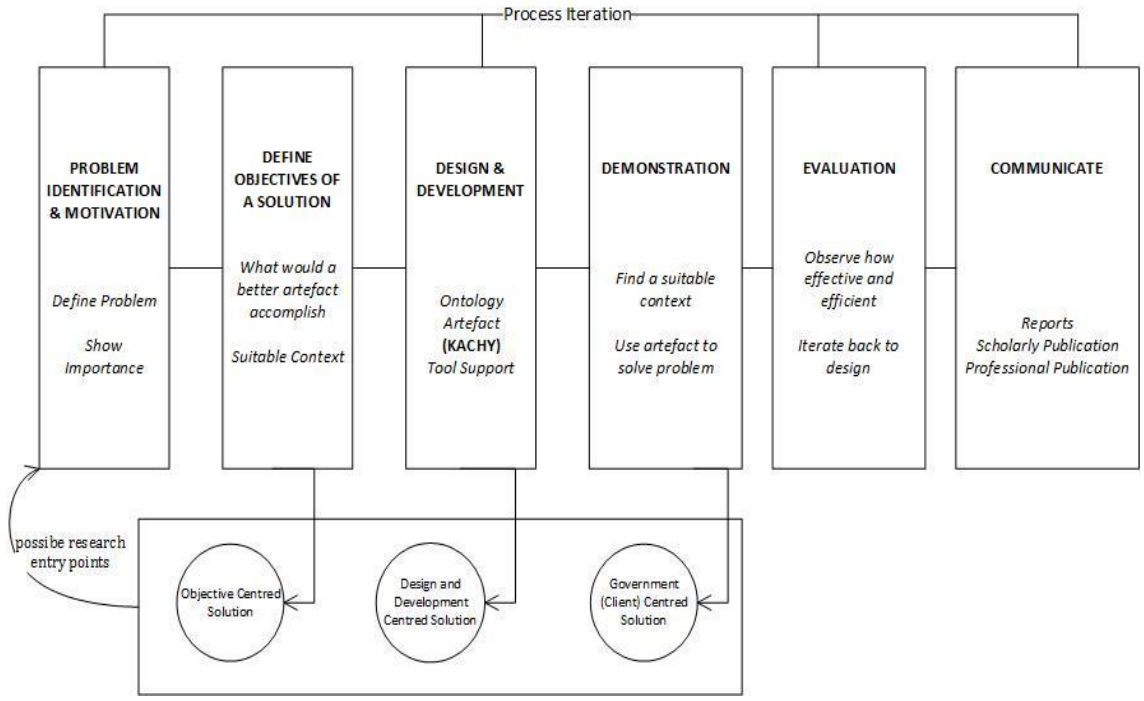


Figure 5. 3: Complete Research Process Diagram (adapted from Peffers et al. 2007)

Table 5. 3: Description of DSR Steps

DSRM steps	**Description**	**Activities involved**
Identification of the problem	This involves identifying the reason for which data is being collected	Literature review searches that discuss the issues surrounding evolution in E-Government. Identification of knowledge gaps stated in chapters 1,2 and 3.

DSRM steps	Description	Activities involved
Definition of the objectives of a solution	This involves designing a framework ontology that is able to model evolution-related relationships while analysing the risks associated with this. This involved an iteration between steps 1 and 2 which leads to the development of objective-centred solution	Semantic modelling with the use of ontologies. Clear objectives of the research stated in Chapters 1 and 2 and justification of tool in chapter 4.
Design and Development	Design of the TRAO model: a framework that can be used by governments to analyse the risks of evolution	The development of the conceptual framework in Chapter 6 provide the basis on which the ontology and tool are developed and designed. This involves the use of Shared services theory, SOA modelling, semantic modelling etc. Functionality of tools are described including the architecture of the framework. This is defined in Chapter 7
Demonstration	The use of the ontology and tool to prove that the reason behind its development is met	The use of defined scenarios and running examples in chapter 7 to ensure that the research objectives are clearly met
Evaluation	Evaluation of the tool to ensure that the tool supports the solution to the identified problem	This involved checking for ontology consistency, completeness, reliability and tool usability. This is presented in chapter 8

DSRM steps	Description	Activities involved
Communication	This involves publications related to this subject to demonstrate the results of the knowledge gotten from this research	The thesis and the publications associated with this research in 1.7 communicate the results of the research

With Design Research, it involves the creation of all or part of the phenomenon as most of the phenomenon is not naturally occurring (Vaishnavi & Kuechler 2015). The relevant end products or IT artefacts of a DSR include the following: models, methods, constructs, instantiations or a combination of these (March & Smith 1995).

The present study is concerned with designing, developing and evaluating an ontology and a tool used in managing the risks associated with evolution in E-Government. A model was developed by Peffers et al. (2007) to show how the research will be designed and how tools and artefacts should be implemented. This design shows how the research process will be completed.

5.7.5 Ontology Development Methodology

The development of the ontology presented in Chapter 7 involved the following steps:

Determination of the Purpose and Scope of the ontology: Identification of the purpose and scope of an ontology limits the ontology developer from including data which may not be relevant to the ontology. This data may be relevant generally but may not play any significant role if included in the ontology. This helps in keeping the number of concepts, relationships and instances to be included in the ontology to the barest minimum especially when analysing the ontology.

Description of the Domain: Describing the domain involves the enumeration of relevant terms in building the ontology as well as application of the principle of having hierarchies within the ontology. This enables the organization of knowledge as well as establishes the granularity of data that should be included in the ontology.

Scenario Formulation: the functionalities of a system are defined using user scenarios so that users can determine what to expect from a system and how to apply it (CEDAR, 2016). Taking into account the opinions of modelling ontology as presented by (Gruninger & Fox 1995), this step was included in the ontology development process. Gruninger and Fox were of the opinion that it is necessary to informally model scenarios that would be motivating in the development of the ontology (Gruninger & Fox 1995). These scenarios they believed show the kind of problems people need information about that the ontology being modelled would not necessarily provide. Scenario formulation helps in narrowing the scope of the ontology as well. Thus, the formulation of scenarios provides an excellent way to get a clear picture of the ontology. Lee (2006) posits that scenarios can be used to support each phase of the ontology development process.

Competency Question Formulation: The formulation of scenarios in (3) led to the development of competency questions. This approach was employed because Uschold (1996) posits that scenarios could serve as a thorough approach of developing competency questions. He pointed out that competency questions are based on scenarios and are able to express different reasoning problems that must be supported. A question may be said to be competent if the ontology can provide supporting answers to the question and serve the purpose for which it was intended (Uschold 1996). The development of the right competency questions would show off the reasoning capabilities of the ontology. Simply put, "*if there is no competency question that requires the use of a term or a concept then that term or concept should not be included*" (Uschold 1996). In their paper, they also stated that no ontology is associated with a set of competency questions but rather the questions are used to evaluate the ontological commitments that have been made to see whether the requirements of the users of the ontology are met by the ontology (Uschold & Gruninger 1996).

Development of Templates for Scenarios: In order to define scenarios and communicate them to those involved, it is a requirement that templates are designed and used.

5.8 Ethical Considerations

The nature of qualitative studies brings about interactions between researchers and participants which can be ethically challenging for the researcher since they are personally involved in different stages of the study (Sanjari et al. 2014). Since qualitative research does not generally involve statistical analysis; evaluations and interpretations had to be made

based on what was read and observed as a trend in the E-Government domain with respect to evolution.

Ethical considerations form a major part of the research as lapses in ethics can significantly harm the subjects of the research. Resnik (2015) defines ethics as *"norms for conduct that distinguish between acceptable and unacceptable behaviour"*.

The ethical considerations need to be adhered to so that the aims of research focussed on truth, prevention of error and authenticity can be adhered to (Datt & Datt 2016). There are many reasons why adherence to ethical norms in research is important. Some of the reasons outlined by Resnik (2015) include: (1) to promote the research aims such as truth, knowledge and error avoidance (2) to promote values such as accountability, trust, mutual respect and fairness which are essential in the research (3) to help in building public support for the research especially when the quality and integrity of a research is not compromised (4) to ensure that researchers are accountable to the public and conflicts of interest are managed (5) to promote a variety of other social and moral values such as human rights, compliance with law, safety and social responsibility.

During the collection and interpretation of data, the following ethical considerations were adhered to:

1. Participants consent were sought before data collection
2. The purpose of the interview was explained to each participant during the in-depth interview
3. Participants were assured of confidentiality during interview
4. Reports, methods and procedures were reported honestly.
5. Bias was avoided during the interpretation of the research.
6. Only published data was used during the hermeneutic phase of the research.
7. Confidential communications were kept during the course of the research
8. Relevant laws and institutional and governmental policies were adhered to

5.9 Conclusion

A detailed account of the philosophical assumptions, the research approach, method, strategy and ethical considerations have been presented in this chapter. Justifications for the data collection methods and strategies chosen were provided. More importantly in this chapter

was the discussion on the IT artefact which shows the potential of its development using the DSR methodology and the development of kernel theories linked to the social sciences. The DSR methodology combines the advantages of different paradigms in its approach. For this research, it has combined the generation of theories gotten based on hermeneutic analysis and the interpretivist paradigm to generate theories out of the created artefact and its usage. The actual work underlying this thesis combined theory, empirical collection of data, analysis and the development of the ontology and tool in an iterative way.

Chapter 6: Conceptual Framework for the Management of Risks in E-Government

In this chapter, the theoretical foundation of this thesis is presented in the form of a conceptual model for understanding the risks that occur as EGov Services evolve and the effect this evolution has. This involves managing the relationships that exist between the E-Government Domain (comprising of EGov Services, SRs, SPs); the Security Domain (comprising of Risks, Vulnerability and Threats); IT Services and Assets. Thus, conceptual knowledge is introduced to overcome the limitations associated with the retrieval of necessary information relating to these domains as well as the formulation of user queries. Furthermore, this chapter presents the use of an ontology as a means to unifying the semantic knowledge produced in the different domains by mapping concepts in the different domains into conceptual models.

6.1 Reasons Behind the Development of a Conceptual Framework

Recent developments in domains such as Risk Management, Systems of Systems, Systems Thinking etc., have led to numerous attempts to apply technological solutions in the E-Government domain. The literature review carried out in Chapters 1-4 reveals a wide range of examples where evolution in the E-Government domain is accompanied by associated risks. Considering that the application and use of technology greatly increases the complexity of E-Government especially in terms of EGov Service delivery, there is the need to develop a conceptual framework for the dynamic nature of E-Government. The proposed framework is based on managing evolution-related risks in E-Government and the ability to manage the IT assets that may be compromised by this evolution. A rationale for context-based reasoning in E-Government is adopted and a conceptual model for evolving risks in E-Government is further developed.

While a variety of theories and ontologies exist for the E-Government, Asset and Security domains, no conceptual framework has been developed so far which hold together the heterogenous and very different entities involved in Stakeholder interactions, Service Provider-Service Receiver roles, relationships, workflows, Assets, events etc. In order to establish a relationship between these entities, appropriate relations must be defined that will be used to govern every possible interaction between these entities. Methods that have emerged from the development of processes within E-Government suggest that the aspect of

E-Government issues intertwined with risk, assets, security issues are separated rather than integrated. Therefore, the use of an integrated method for developing this domain should lead to the simultaneous optimization of efficiency and processes.

6.2 Proposed System

The first step taken in developing a system suitable for the given domain is to develop an ontology that conceptualises the terms associated with the different domains (as discussed in Section 6.1) and unifies them through their relationships. The use of an ontology-based approach is proposed so that assumptions can be stated explicitly, results can be retrieved accurately and further understanding can be generated based on the generation of inferences. The proposed ontology-based approach for managing evolution risks in E-Government will be designed in such a way that a user can interface with the system (tool) using a web-based interface and can get information that is relevant to their queries. Furthermore, a user can use the web-based tool to look up relevant information as well. Thus, allowing for relevant decisions to be made. The Threat Risk Asset Ontology (TRAO) system has as its main objective the development of a model for E-Government that facilitates the management of evolution risks as a means to managing assets. It will be responsible for handling the retrieval of information, matching information semantically as well as providing results based on inferences that have been generated in the ontology. Thus, the use of an integrated approach as proposed in Section 6.1 will be a major contribution to the research.

6.2.1 Development of a Five-Level Model of the E-Government System

In order to develop a conceptual framework for E-Government, a five-level model for the E-Government system is developed. This is based on the need to provide structure and clarity in the E-Government domain as well as understand the challenges that E-Government faces. The model developed in relation to this research is divided into five different nested levels which are: (1) EGov- Service, (2) IT Service, (3) Assets, (4) Stakeholders, (5) Risks.

Figure 6. 1: Five Level Model of the E-Government System

EGov Service: The core of the model is the EGov Service layer which is the major defining factor in any EGov System. Chapters 1, 2 and 3 established how changes in E-Government have an effect on the delivery of EGov Services and how efforts are constantly being made to improve EGov Services. The improvement of EGov Services should be accompanied with a change in perspective to consider the IT Services, Assets, Stakeholders and more importantly the risks associated with these processes. Thus, there should be a synchronous communication that exists between the different layers of the model and the EGov Service to manage these effects of change.

IT Service: The second layer of the model shows IT Services. This layer consists of core services, supporting and enhancing services responsible for supporting EGov Services. These have been discussed extensively in Chapter 3. It is responsible for responding to user requests. An IT Service is required for an EGov Service to run. It is also responsible for initiating the assets on which an EGov Service will eventually run. Thus, the rules of engagement between EGov Services, IT Services and assets are established.

Assets: The third layer of the model is the asset layer. The asset layer is responsible for supporting the delivery of EGov Services. These include systems such as systems of systems, operating systems, decision making systems, infrastructures, platforms, etc. It has also been established in chapter 2 that assets are made up of components. Thus, the effect of the

influence of asset components must be taken into account and a logical understanding of the relationship that exists between assets and asset components is taken into consideration.

Stakeholders: This is the fourth layer of the model. Stakeholders are critical to the smooth running of EGov Services and are equally under pressure to be at par with evolutionary changes. Thus, they are susceptible to risks as well. Given that the EGov system may be seen as a highly fragmented system (Singh, 2015), stakeholders must be supported in knowing what assets are in use and the effects the use of an asset may have on them and the delivery of EGov Services.

Risks: This is the fifth and last layer of the model. This layer is presented to show that with each of the other layers (1-4) come associated risks. The other levels of the model are responsible for influencing risks in the EGov system.

6.2.2 Unified Conceptual Framework

This section presents an overview of the unified conceptual architecture that is responsible for implementing the main features of the proposed system that has been presented in Sections 6.1 and 6.2. One of the first tasks during interactions with key stakeholders was the development of a conceptual framework to assist stakeholders in developing and interpreting operations of asset-related evolution risks within the E-Government domain. The objective behind the development of this conceptual framework was to create a foundation that is consistent and one that covers the major areas of discourse as it relates to the project.

The TRAO system would contain a look up option that enables stakeholders identify the different relationships that exist between Stakeholders as well as assets. Furthermore, this look up tool will provide relevant information on security issues such as risks, vulnerabilities, threats and associated impacts. A major feature of the TRAO system is TRAOSearch which is responsible for allowing searches and queries to be made. Based on the metadata details provided, the TRAOSearch engine retrieves data/information that is directly related to a query that has been specified as well as other relevant information based on inferences that may be generated by the TRAO. Figure 6.2 provides an overview of the conceptual framework.

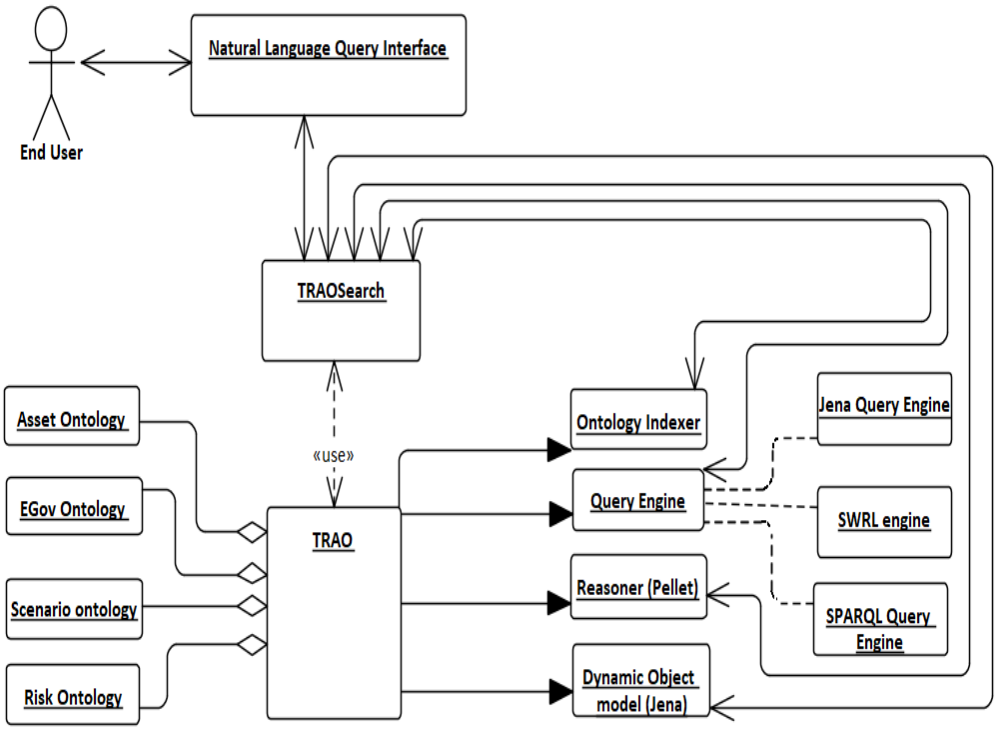


Figure 6. 2: Overview of the TRAO Unified Conceptual System Framework

The operation of the conceptual framework is as follows:

1. User/Query/Result Interface module: this would enable a user query and see results of the query as well as perform searches. Users can run queries using natural language.
2. Combined ontology module: This is made up of the ontologies and the model frameworks that make up TRAO. This combined ontology module serves as a knowledge pool. They are individually discussed in section 6.3. Sections 6.3.1 and 6.3.2 provide the EGov ontology framework; Sections 6.3.3 and 6.3.4 provide the Asset ontology framework; Sections 6.3.4; 6.3.5 and 6.3.6 provide the risk framework as well as a scenario framework. Figure 6.16 shows the high-level view of the ontologies that have been developed to form the TRAO.
3. Query module: this module is responsible for retrieving relevant information for a user. When a user enters a query, the entire ontology is traversed to match the concepts, property, keywords, sub concepts or instances. If these terms match what is in the ontology, then an inference can be made from them.

4. Ontology matching/indexing module: This is responsible for deriving variants of the same idea. For example, the word "provide" can have the following variants: "provides", "provided", "providing".
5. Triple store module: the use of Jena to generate the combined ontology (TRAO) into triples as well as produce a dynamic object model.

6.3 Development of a Conceptual Framework

Jabareen (2009) defines a conceptual framework as *"a network, or "a plane," of interlinked concepts that together provide a comprehensive understanding of a phenomenon or phenomena".* A conceptual framework is not just a visual model of the main concepts of a researcher's theory. Although this chapter presents visual models of top level concepts, it is accompanied by information regarding the connections that exist between the concepts.

The definition of a working conceptual framework for this research is founded in four bodies of knowledge: the problem of managing risks associated with evolving EGov Services; the use of IT governance frameworks; the problem of managing assets that may be affected by evolution; and the use of models and ontologies as tools for mapping assets to SPs and managing the relationships that exist between them. This section handles the description of concepts surrounding TRAO separately which is linked to the unified model that has been presented in section 6.2.1. This section also focusses on extracting and mapping the main concepts identified and discussed in the preceding chapters (1-4). This involves identifying the relationships that exist across each major area of discourse and showing their interconnectedness. This section presents efforts to understand how EGov Services evolve and the effects of this evolution in terms of risks. Thus, efforts to understand how EGov Services evolve and the risks associated with this evolution are presented by unpacking EGov Service into four dimensions:

i. as a service made available by SPs to SRs;
ii. as a service that is dependent on the operations of IT Services;
iii. as a service whose dependence on IT Services involves the use of assets;
iv. as a service capable of evolving and being at risk

At the core of the theoretical foundation of this research, the main concepts identified are: ***E-Government, E-Government Service, Asset, IT Services, Risk, Stakeholder, Evolution.***

The concept of E-Government is used as the starting point for discussions in this area. As represented in this thesis, the concepts of E-Government and EGov Service are related and overlapping concepts involving other aspects of research. Although the development of E-Government and EGov Services are greatly related to the field of information sciences and technology which is seen to be existent in organisations; there is the need to accommodate various strands of critical understanding. This encompasses a broad range of theoretical standpoints, views and a combination of practical applications with theory to offer a source of reference that is valuable.

The E-Government domain is enmeshed in complex interactions with complex systems that are constantly evolving. Thus, as attempts are being made to improve the processes involved in service delivery, these are being hampered by the undesirable effects they may have on other systems. However, the effects of these are not just on the systems alone but also across service providing organisations. In the words of (Sterman, 2012), *"the consequences of our actions spill out across time and space and across disciplinary boundaries, our universities, corporations, and governments are organized in silos that focus on the short term and fragment knowledge".*

This research examines the relationships that exist between the organisations in government in which they are embedded and the existent information systems. It identifies the need to examine and assess the ways in which the evolution of assets generally affect service providing organisations and the effects this has on service provisioning. A critical approach is taken to analyse this to show that there is the possibility of new research arising if the approach for analysis shifts from a positivist or interpretivist to a critical approach. Thus, a working overarching conceptual framework is defined to enable the definition of such relationships and their effects in the form of risks.

6.3.1 Development of Framework based on Theories of E-Government

Chapter 2 discussed the different viewpoints held by different authors about E-Government. In this thesis, E-Government is understood to be an evolutionary process. This process involves the provision of EGov Services with technology acting as an enabler which has the potential to provide new ways of thinking of processes and organisations involved in service delivery. However, the emphasis on the use of technology in government highlights several issues associated with the provision of EGov Services. The use of digital technologies is challenging the effectiveness of policies that were previously developed and the Tallinn

Declaration on E-Government discussed ways in which these challenges can be managed to meet the expectations and needs of citizens and businesses (European Union 2017; Ministerial Declaration on eGovernment 2009). Some of these ways which apply to this research include:

i. increasing the transparency, responsiveness, reliability, and integrity of public governance;
ii. improving the conditions for the interoperability of administrations;
iii. the need to increase the efficiency and effectiveness of governments so that the administrative burden is reduced, and organisational processes are improved;

The emphasis on *"improvement"* and *"increase"* highlights the role technology plays in government. The dimensions of discussion presented in chapter 2 on E-Government set a point of departure for a meaningful description of E-Government. Thus, a meaningful description of E-Government can also be achieved by discussing it in terms of the salient features of E-Government such as:

1. ***The IT artefacts that make up E-Government and the structural dependencies that exist between these artefacts;***
2. ***The relationships technological evolution has with E-Government;***
3. ***The systems or processes the IT artefact in E-Government is connected to;***
4. ***The characteristics of E-Government that correspond with technology discussed by stage models;***
5. ***The assets required to enhance the relationship between evolution and EGov Services;***
6. ***The risks enmeshed in this relationship as stated in (5).***

Considering that this thesis seeks to address the issue of evolution in government, maturity models serve as a guide to enable the reader to understand the progress that has been made so far in the E-Government domain and whether the models are still relevant to the evolving needs of government. Based on existent E-Government models, there is a consistent reference of the development of E-Government using technology at different stages.

The stages of previously developed E-Government models such as: Layne and Lee model Layne & Lee (2001)**,** Baum and Di Maios model Baum & Andrea Di Maio (2000)**,** ANAO model (Persson & Goldkuhl 2005; Australian National Audit Office 2000) are developed to

reflect some of the dimensions that technology/digitalisation plays in the development of E-Government. However, as pointed out by Persson & Goldkuhl (2005), these evolutionary stages are not mutually exclusive or absolute. Thus, these may require deliberations on behalf of the analyst when applied or analysed with concepts of E-Governments. Hence, this study has necessitated the introduction of artefacts (A1, A2 and A3) related to E-Government and a risk evolution stage.

{A1} E-Government ⟶ Dynamic Relationships between Artefacts

The development of dynamic artefacts is in line with the relationships that exist between the different types of Government (G2B, G2C, G2G) and the different relationships that exist between IT Services and EGov Services.

{A2} Eliminate manual process ⟶ Provides digital service

This is in line with eliminating repetitive and manual processes while providing services that reflect present-day modern government (Public Governance and Territorial Development Directorate 2014; National Audit Office 2017a).

{A3} Providing digital service ⟶ Manage associated evolutionary risks

As efforts are ongoing to provide digital/electronic services in ways that eliminate processes that are manual and repetitive whilst providing services that reflect present-day modern society, it is equally important to analyse the risks that may emanate from digitalising government (Public Governance and Territorial Development Directorate 2014; National Audit Office 2017a). This is also in line with the E-Government Reference model developed by Samarin (2014) where technology is increasing processes in E-Government with effects that are good and bad. Based on the questions answered and the knowledge provided by this, this provides a guide to identifying EGov Services and analysing their characteristics in relation to the role they play in E-Government.

Thus, the introduction of artefacts (A1, A2 and A3) has necessitated the development of an E-Government framework which is grounded on the artefacts that make up E-Government, the relationships that exist between the artefacts as well as the risks enmeshed in the relationships. The evolutionary aspect of the framework is presented in a structural diagram shown in Figure 6.3. It shows how the use of technology encourages evolution which end up in evolution risks.

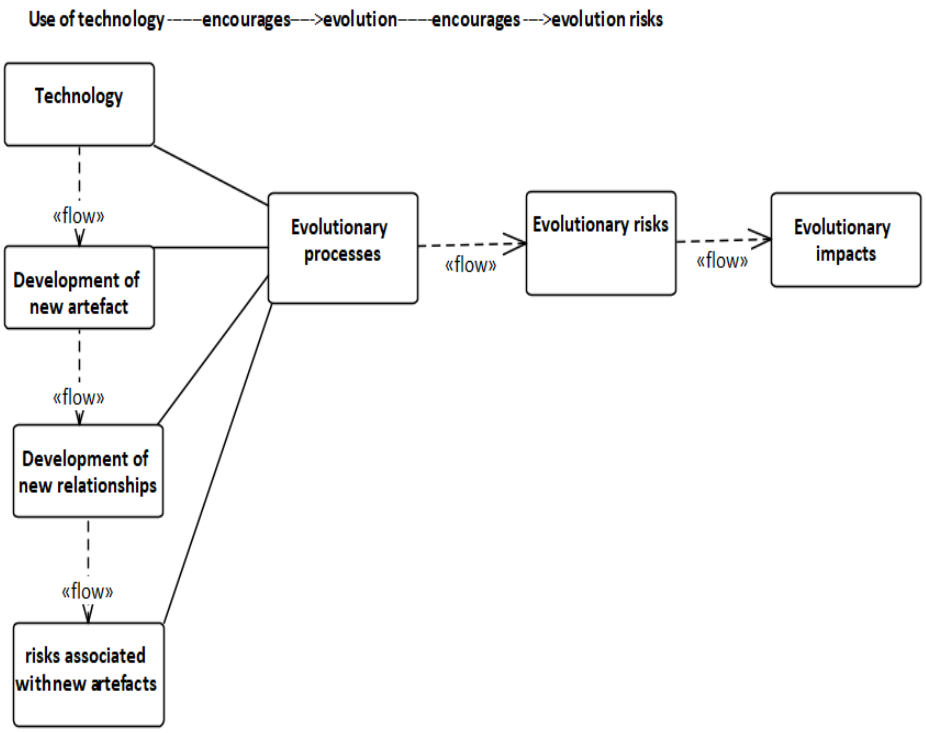


Figure 6. 3: Structural Diagram Showing Evolutionary Aspect of E-Government Framework

6.3.2 Development of a Framework based on the Existence of E-Government Stakeholders

The goals behind the development of E-Government that extend to stakeholders are partly overlapping and cover a different set of stakeholders. This section takes into consideration the roles of the two main stakeholders (SR and SP) in government. A use case diagram showing the basic activities of these stakeholders is presented in figure 6.4.

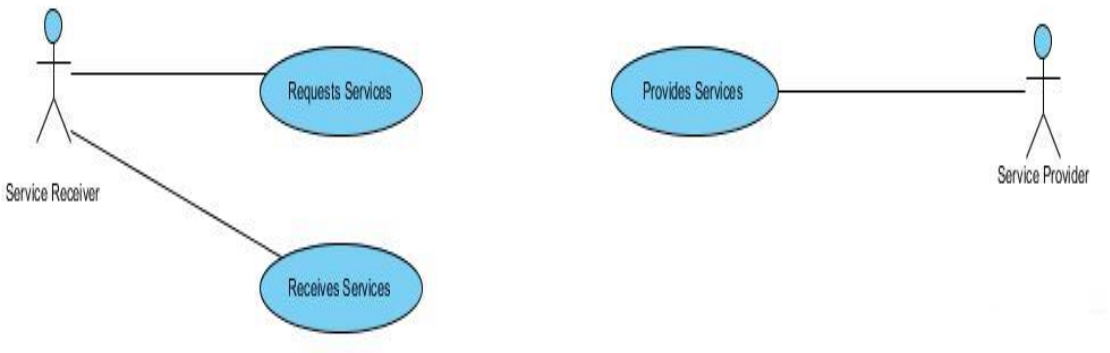


Figure 6. 4: Use Case Diagram Showing the Relationship between Services and Stakeholders

The SR use case describes the interactions a SR has with the E-Government System. The SR can request for EGov Services and can also receive EGov Services.

The SP is responsible for the provision of EGov Services. The SP uses the system as an active actor by interacting with the E-Gov System. Thus, he initiates the execution of use cases. While the active/primary actor in this case (Service Provider) gets a direct benefit from the execution of the use case, the E-Government System gets no direct benefit from the execution of the use case.

Figure 6.5 presents a use case of the two main stakeholders in government. However, the SP use case actor can also act as a SR by requesting for an E-Government Service. This is seen in cases where a SP can be making a request from another SP but acts as a SR in that instance.

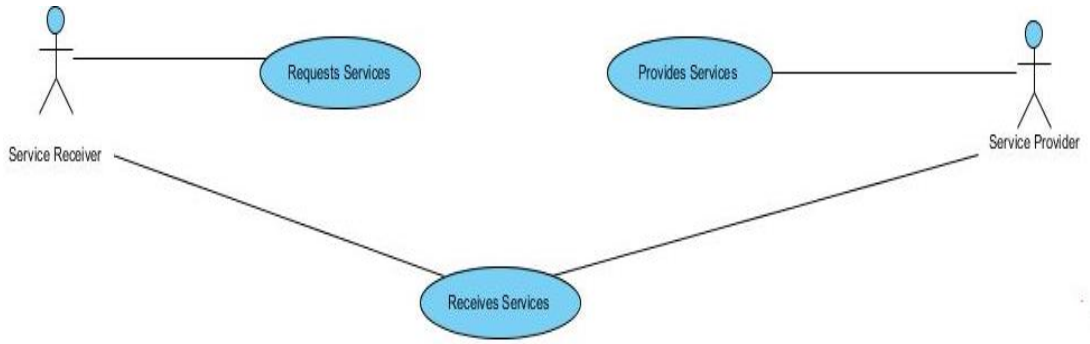


Figure 6. 5: Use Case Diagram, Showing the Relationship between EGov Service and SRs

6.3.3 Development of a Framework based on the Composition of Assets

In preceding chapters, it has been established that assets do not exist on their own. A group of components make up an asset. A typical Asset (AS1) may be made up of components with different dependencies. Figure 6.6 presents a sample component diagram showing the kind of dependencies that may exist between assets in E-Government. It shows that an EGov Service requires an asset and an asset can be made up of components (AC_1, AC_2, ----, AC_n). Furthermore, as previously established in Sections 2.3.4 and 3.4.3.1, an asset can have different relationships that may exist in the form of dependencies even amongst its component parts.

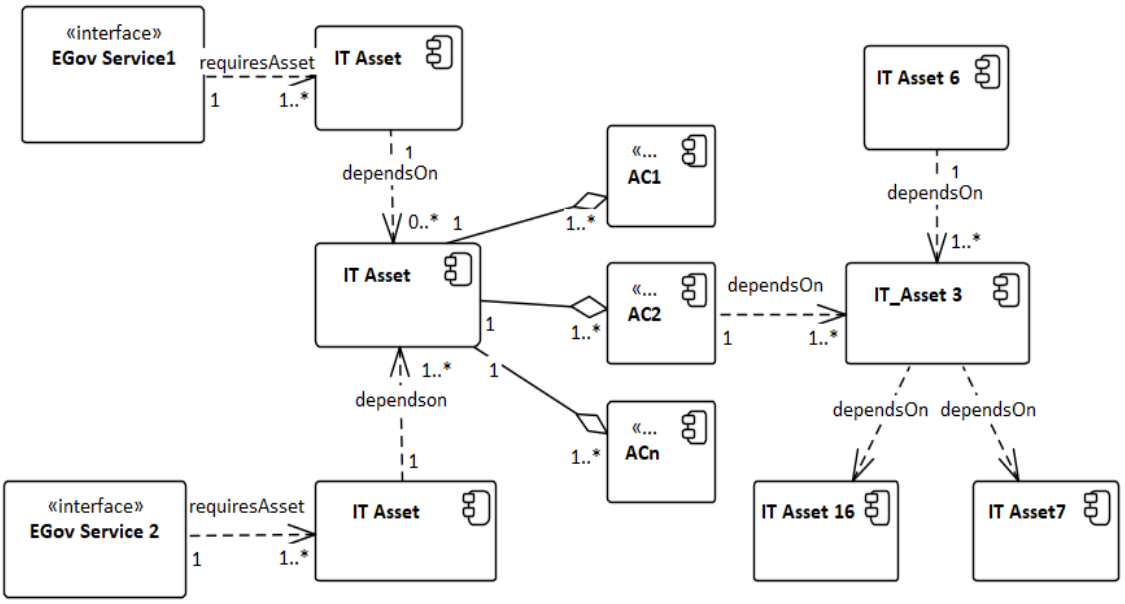


Figure 6. 6: Overview of Dependencies that Exist between Assets

6.3.4 Development of a Framework based on an Asset-Based Approach to the Management of Risks

This section presents an asset-based approach to the management of risks in government. An integrated approach to managing IT assets in government is presented with risk management strategies.

The asset-based approach presented in this thesis uses a broad definition of Assets which categorises assets based on their types such as Hardware assets, Software assets, critical assets, reusable assets etc. Section 3.6 also discusses the management of assets using a risk-based approach. This presents the different types of risks that IT assets are exposed to. The definitions of risk are also provided in section 3.6.

There are different ways that an asset can interact with a risk. This could be in terms of the source of the risk, the targeted asset of the risk, the impact of the risk etc. Risks are spread across governments using assets as their entry point. Another interaction level is seen in the reallocation of assets if there is a failure of an asset. Thus, a backup asset can be introduced within the E-Government system as a way to respond to a risk. Assets and risk are closely linked because risk is transmitted through the E-Governments asset portfolio and assets are allocated to also manage these risks.

This asset-based approach is concerned with how governments can break out of the evolution cycle if an asset is at risk of failing. This has incorporated the use of several terms that have been used to emphasize the dynamic approach to managing assets associated with evolution in government. These terms are closely related to the concept of vulnerability and threat. Vulnerability in this case may be explained as the probability that there may be the loss of a critical service or a system compromise given that there is a risk. Thus, it is important to know the source of a risk, the impact of this risk, how this risk can be mitigated and what security objectives are compromised if there is a risk. Figure 6.7 provides the asset-based approach to the management of risks within E-Government. The diagram shows that security mechanisms reduces the probability of the occurrence of risks and threats. An asset is always the target of a threat which is exploited by a vulnerability. Also having the right security mechanisms in place protect an asset.

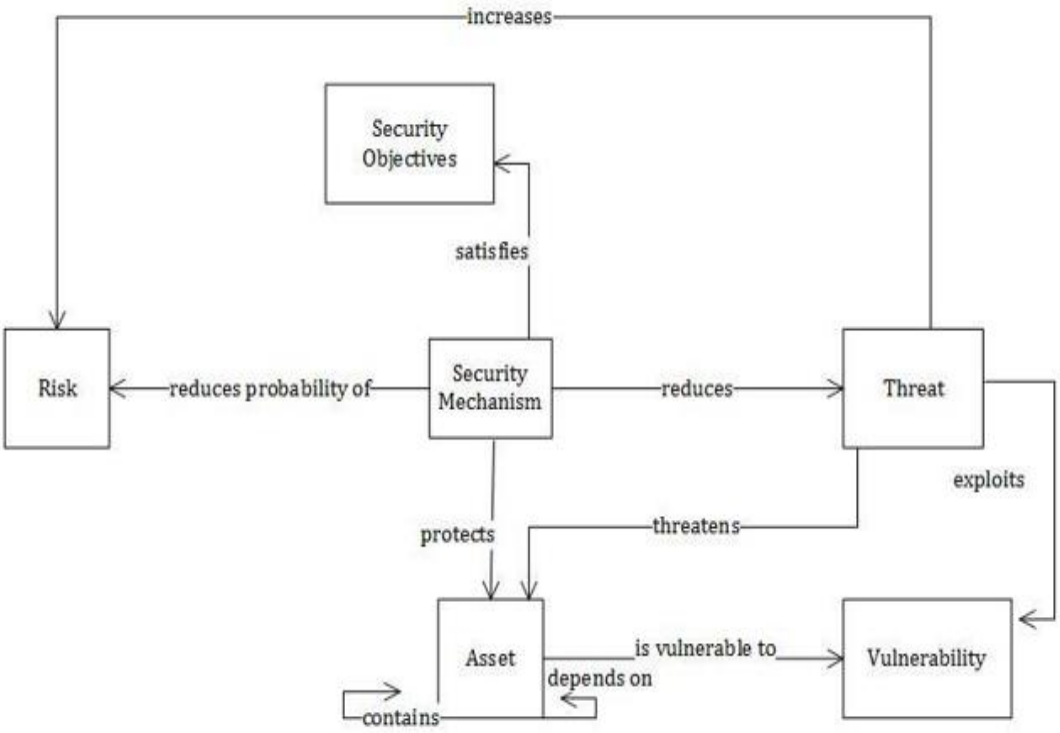


Figure 6. 7: Block Relationship Diagram Showing Asset-Based Approach to Risk Management

The diagram also shows that an asset contains an asset. This means that other assets may be embedded in an asset as shown in Figure 6.6. This supports the definition of an IT artefact provided by Benbasat & Zmud (2003) which includes the aspect of an artefact being

embedded in another artefact. It is important that the most critical assets and the risks they are susceptible to are identified. A risk framework is presented in Figure 6.8.

6.3.5 Development of a Framework Based on the Risk Structure

The relationships that exist between assets is likely to increase the risks associated with them. This is because from figure 6.7, an asset depends on an asset. Understanding the dependencies that exist between assets is critical to the assessment and management of risks. Figure 6.8 presents a risk taxonomy diagram and the relationships that exist between a risk and other high-level classes. A description of the figure 6.8 is shown in Figure 6.9.

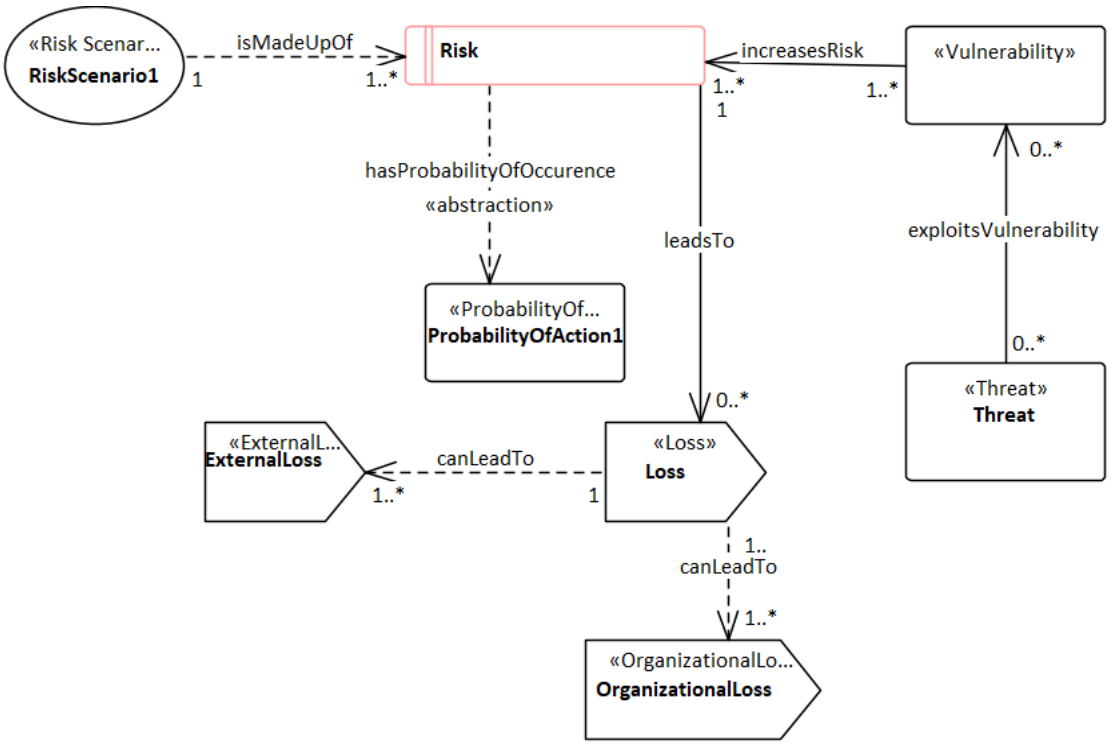


Figure 6. 8: Risk Structure

1(Risk Scenario) *isMadeUpOf* 1…* (Risk) shows that 1 risk scenario can be made up of 1 to many risks;

1...* (Vulnerability) *increasesRisk* 1...* (Risk) shows that 1 to many vulnerabilities can increase 1 to many risks;

0...* (Threat) *exploitsVulnerability* 0...*(Vulnerability) shows that no threat or many threats can exploit no vulnerability or many vulnerabilities;

1 (Risk) *leadsTo* 0…*(Loss) shows that 1 risk may lead to no loss at all or many losses;

1(Loss) *canLeadTo* 1…1..*(ExternallLoss) shows that 1 loss can lead to 1 to many external losses;

1(Loss) *canLeadTo* 1…1..*(OrganisationalLoss) shows that 1 loss can lead to 1 to many organizational losses.

Figure 6. 9: Description of Figure 6.8

6.3.6 Development of a Framework based on the Management of Evolution-Related Risks in E-Government

Carney et al. (2005) defined evolution as *"any change in the quality, functionality, or implementation of the services offered by a system".* Although many other definitions of evolution exist, the attendant research in this field is concerned with evolution in terms of assets and the impacts it has on EGov Services. However, of significant importance to this research are the 8 laws of evolution developed by Lehman (Lehman 1978; Lehman 1974). For this research, the 1st, 2nd and 6th laws are of most relevance.

The 1st law addresses continuing change and reads thus – *"An E-type system must be continually adapted else it becomes progressively less satisfactory in use".* This law suggests that for a real-world system, evolution is unavoidable. This issue of change has been addressed in the introductory chapter where the reasons for change were mentioned.

The 2nd law addresses increasing complexity and reads thus – *"As an E-type system is evolved, its complexity increases unless work is done to maintain or reduce it".* It has been established in Chapters 2 and 3 that the E-Government domain is a complex one and as such, the interconnections between assets add to this complexity. Thus, evolution of one system/asset may lead to the evolution of corresponding assets.

The 6th law address continuing Growth and reads thus – *"The functional capability of E-type systems must be continually increased to maintain user satisfaction over the system lifetime".* In line with the reasons for the development of E-Government which have been addressed by the Tallinn Declaration on E-Government, governments need to advance their operations to meet up with the demands of citizens. Thus, with this advancement, comes evolution.

In addition to these laws, discussion on evolution in this research is focused on the ways Governments try to adopt innovative solutions to problems and in turn find themselves enmeshed in transformative pressures. Thus, they evolve towards more complexity that comes with associated risks. EGov Services evolve as well as the assets associated with the delivery of these services. The E-Government model on evolution developed by Janowski (2015) is used as a vantage point for the discussion on evolution in E-Government. Evolution in government is grounded in the discussion on stages of E-Government. It is also assumed

that each stage builds on the previous stage in terms of sophistication. This is presented in Appendix IV.

Analysis of evolution can also be approached from a Systems of Systems perspective. In section 3.4.3, assets were analysed in terms of their composition as systems of systems. Understanding the part of an asset that evolves is critical to the design of the system; understanding the reasons for its evolution are also critical to the stakeholders in government. Of more importance is knowing and managing the risks that are associated with this evolution.

The concepts involving the assessment and management of risks in E-Government form the foundation for developing a risk dimension in any E-Government project (Choudhari et al. 2007; HM Treasury 2004; OECD 2014). The approaches employed in the management of risks in E-Government were discussed in Section 3.5.

6.3.7 Developing a Framework based on the Types of Relationships in E-Government

This thesis acknowledges the need for an evolutionary design approach in analysing the risks associated with evolution in E-Government. It has also been established in the preceding chapters that with evolution in E-Government, assets evolve. By this evolution, assets and components are subject to evolution. Carney et al. (2005) examined the evolution of systems that are interoperable and how interoperability can be maintained even as individual systems evolve.

This thesis also recognises the fact that E-Government Services may be interoperable and that there are many cases of the existence of interoperability. Again, the importance of this is seen in the analysis of the different types of interoperability associated risks. For clarity purposes, interoperability is the process of making an application or equipment work with another directly without the specialised input from the end-user (Sherif 2010). Based on this research, different types of interoperability relationships have been developed. This is also applied to the relationships that exist between IT Assets as well. Although these defined relationships are independent of evolution, they raise potential evolutionary concerns.

Case of SP providing EGov Services to other SPs.

1. **Transitive relationship**

SP1 provides service to SP2 and SP2 provides service to SP3. Therefore, it is concluded that SP1 also provides service to SP3. This is a case where SP1 relies on SP3 through SP2.

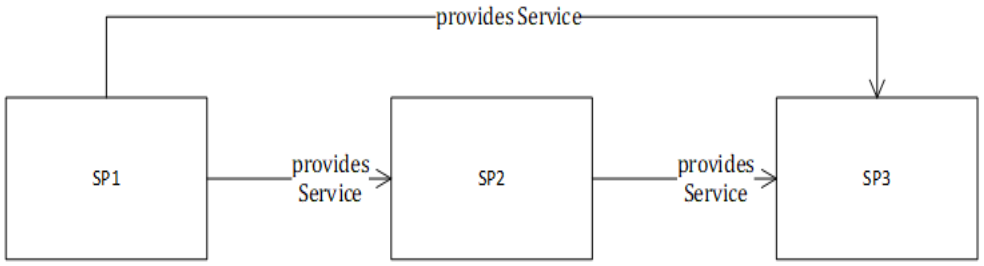


Figure 6. 10: Block Diagram Showing Transitive Interoperability Relationship between SPs

2. **Specialised transitive interoperability relationship**

SP1 provides service to SP2 and SP2 provides service to SP3 without SP1 providing any service to SP3

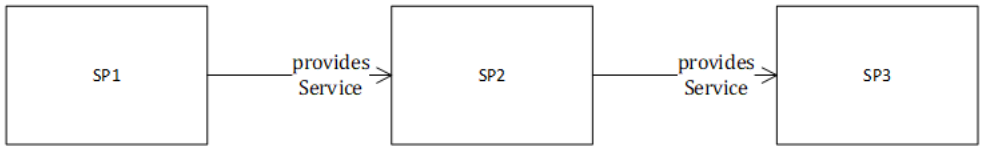


Figure 6. 11: Block Diagram Showing Specialised Transitive Interoperability Relationship

3. **Specialised transitive interoperability relationship with symmetrical relationship**

SP1 provides service to SP2 and SP2 provides service to SP3, SP3 in turn provides service to SP2

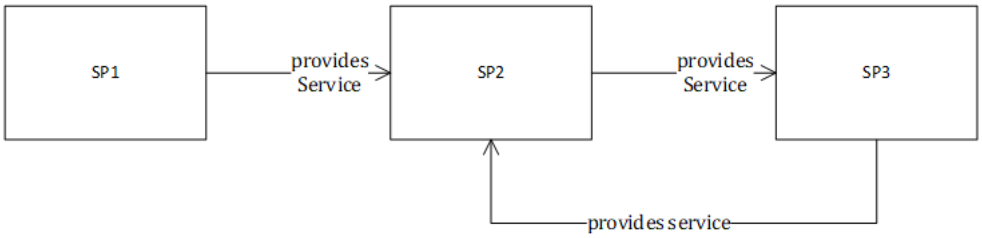


Figure 6. 12: Block Diagram Showing Specialised Transitive and Symmetrical Relationship

4. Specialised forward and backward transitive relationship

SP1 provides service to SP2 and SP2 provides service to SP3, SP3 in turn provides service to SP2 and SP1

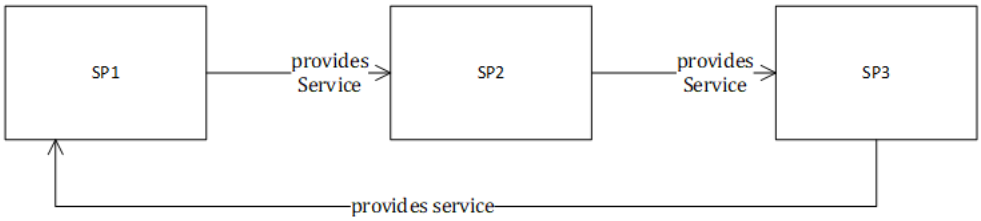


Figure 6. 13: Block Diagram Showing Specialised Forward and Backward Transitive Relationships

5. Symmetric relationship

SP1 provides service to SP2 and SP2 provides service to SP1.

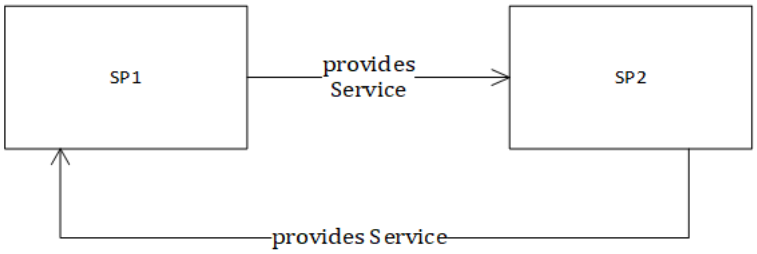


Figure 6. 14: Block Diagram Showing Symmetric Interoperability Relationship between SPs

6. Reflexive relationship

SP1 provides service to SP2 without SP2 providing a service to SP1

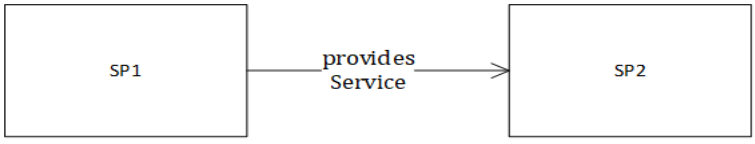


Figure 6. 15: Block Diagram Showing Reflexive Relationship

6.4 Development of the TRAO Framework

This section describes how the individual frameworks for the key concepts of discourse presented in preceding chapters are combined into a single framework. The development of the TRAO framework is based on the conceptual framework which has been presented in Section 6.3. The main part of the framework is made up of a set of ontologies and application scenarios in Section 6.5. The scenarios are used in the context for which the TRAO was developed. Amongst the category of scenarios developed, four major categories of the application of the ontology are considered. These include: Query formulation; Asset search; Asset composition; risk management. There are different scenarios that apply to these four broad areas. In the aspect of asset search, an asset can be searched for based on its relationship to an EGov Service, based on the availability of backup assets, based on its composition etc. Thus, different variations of these scenario categories can exist.

Despite the advancement in technology and in the E-Government domain, there has been a lack of frameworks for developing an ontology-based E-Government tool that is focussed on managing risks associated with evolution. Thus, a framework for managing risks as assets evolve is developed so that the risks associated with different evolution scenarios can be used successfully for studies arising in the E-Government domain. The methodology for developing the framework consists of the following:

1. Capturing of knowledge relevant to TRA
2. Development of an ontology model of the TRA system
3. Implementation of the TRA system
4. Integration of the TRA knowledge with TRAO system

The TRAO framework describes a set of scenarios that help in managing evolution risks in E-Government. The development of the framework is based on the use of the TRA domain ontology as an input. This ontology is developed as a semi-formal version and is created with the use of Protégé. This ontology captures relevant concepts and relationships between the key concepts as shown in Figure 6.17. The creation of instances and relationships between entities in the ontology is carried out.

Ontologies have been presented in chapter 4 as consisting of classes, relationships and attributes. Figure 6.16 presents a data flow diagram showing the ontology modules that make up the TRAO.

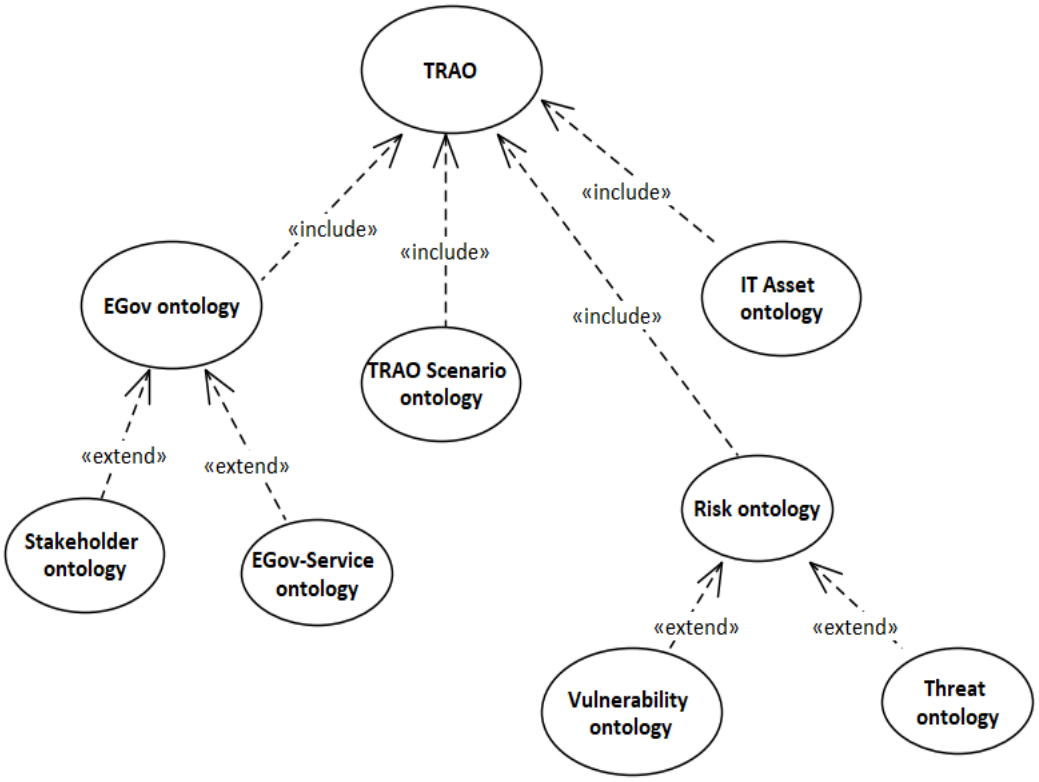


Figure 6. 16: Data Flow Diagram Showing TRAO Components

The description of different models individually sets the background for the description of a general ontology model where new relations are also presented. Figure 6.16 presents the high level conceptual framework of the TRAO consisting of classes, relationships and attributes that exist in it.

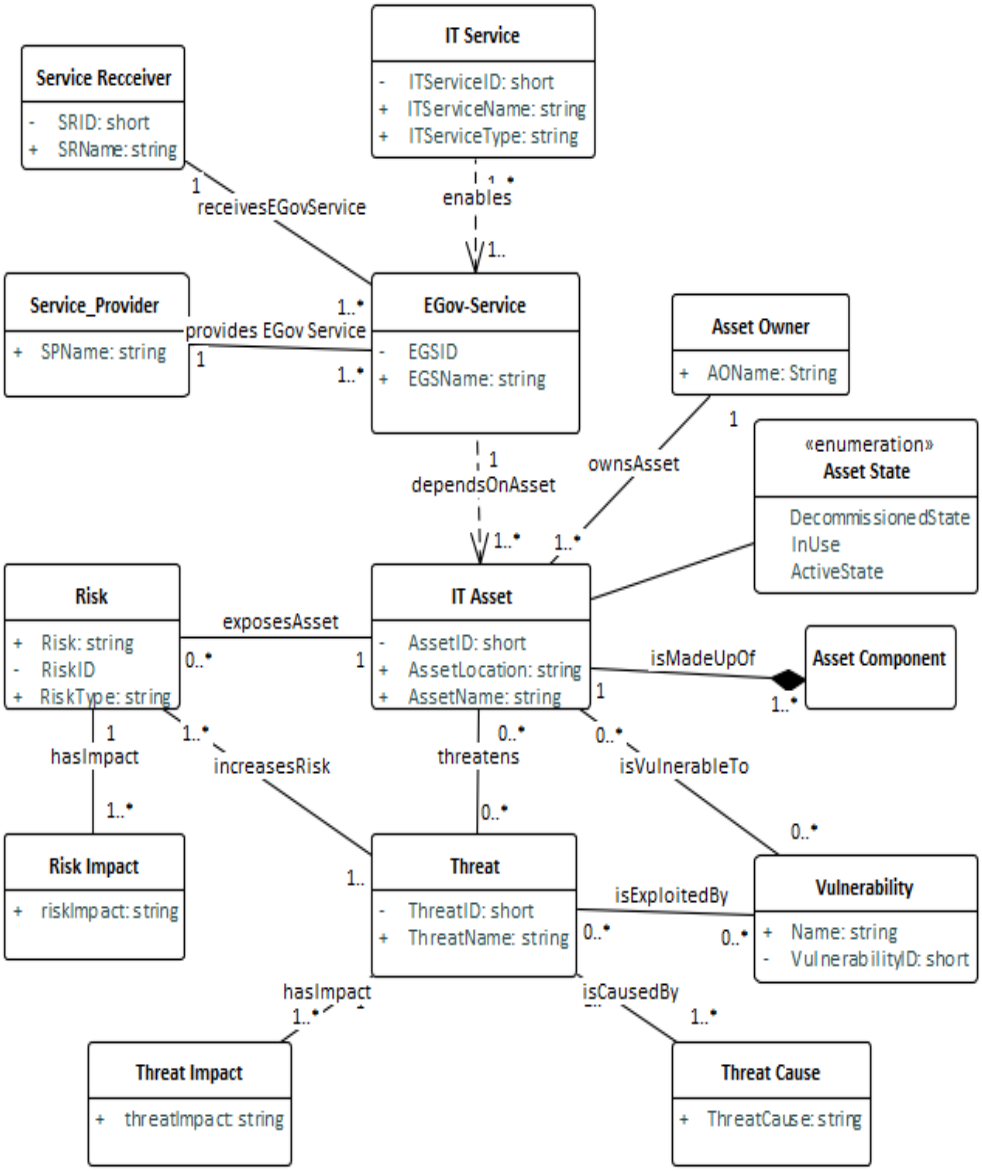


Figure 6. 17: Ontological Conceptual Model for Terms Relating to TRAO Definitions

6.4.1 Service Request Workflow

Figure 6.18 presents an overview of the general E-Government System/framework developed in this research in relation to requesting for an EGov Service. The process begins with a service request made by a SR. This service request is received by the E-Government System which sends the request to the corresponding IT system requesting for an IT service to fulfil the EGov Service request. The IT system immediately initiates a request for IT assets that will be responsible for fulfilling the IT Service needed to fulfil the EGov Service request. Once a response on the availability of IT assets is received by the IT system, the E-

Government System receives results on the availability of the IT services which in turn sends a combined request to the SR, thus providing the EGov Service/ fulfilling the request.

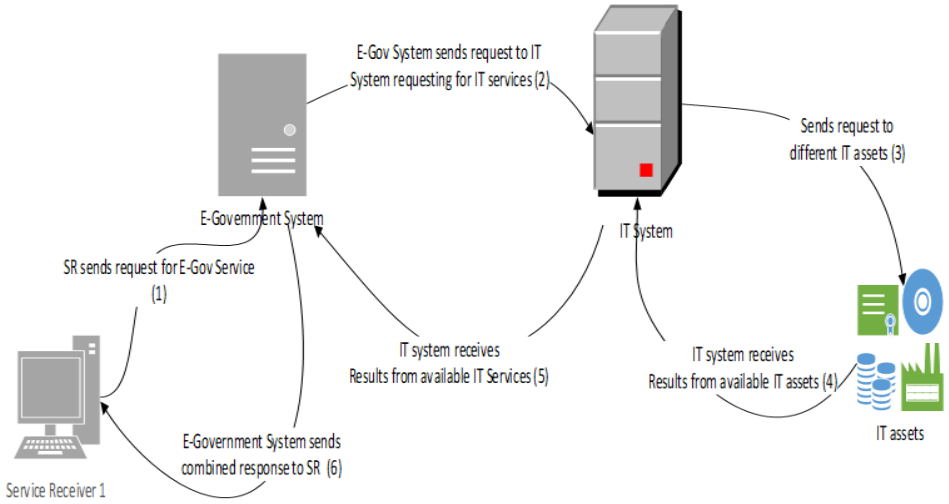


Figure 6. 18: Overview of the Operation of the E-Government System

6.5 Development of Scenarios Relevant to the Thesis

This section describes different use cases relevant to this thesis. Additional example use cases are presented in Appendix III. However, the core use cases are discussed in this section.

6.5.1 Query Selection

Figure 6.19 presents an example use case for performing queries on the framework. A detailed breakdown of the framework is presented in Chapter 8. However, a brief description of Figure 6.19 shows how a user selects requests to formulate a query using the user interface, the queries are sent off to the TRAO query engine (1) which sends off the users queries to the ontology (2). The ontology returns results based on defined rubrics/rules in the ontology which is sent back to the user in (3) and (4). Returned results can be further modified (5) and sent back to the ontology via the web-based query system (Repeating steps 1,2,3 and 4) and final query results are returned to the user (6 and 7).

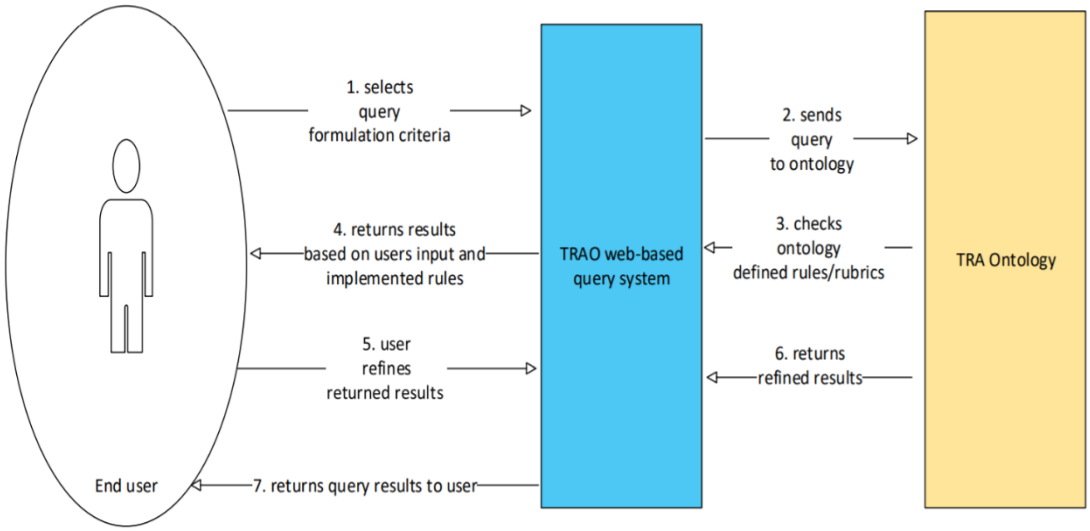


Figure 6. 19: Overview of the TRAO Query use Case

6.5.2 Asset Search Use Case Scenario

Figure 6.20 shows a use case scenario of the search process for an asset to be used.

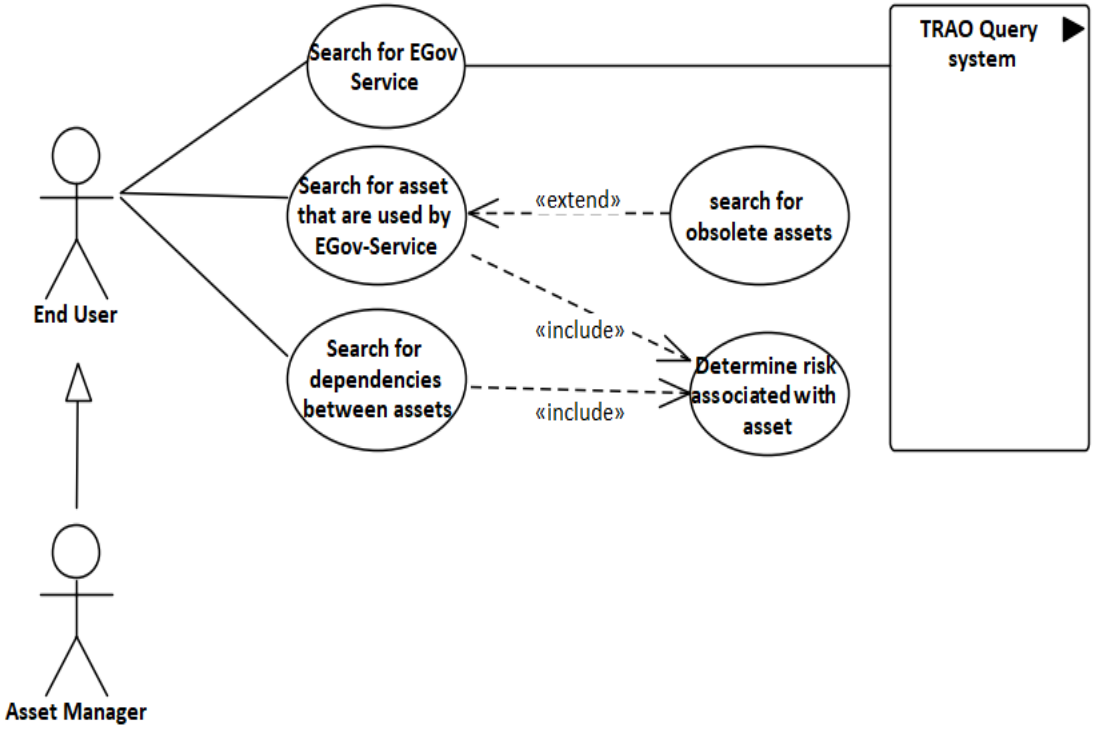


Figure 6. 20: Use Case Scenario of Asset Search

6.5.3 Use Case Scenario for Management of Risk Associated with Assets

Figure 6.21 shows a use case scenario for the identification and management of risks. More example use case s are presented in Appendix V.

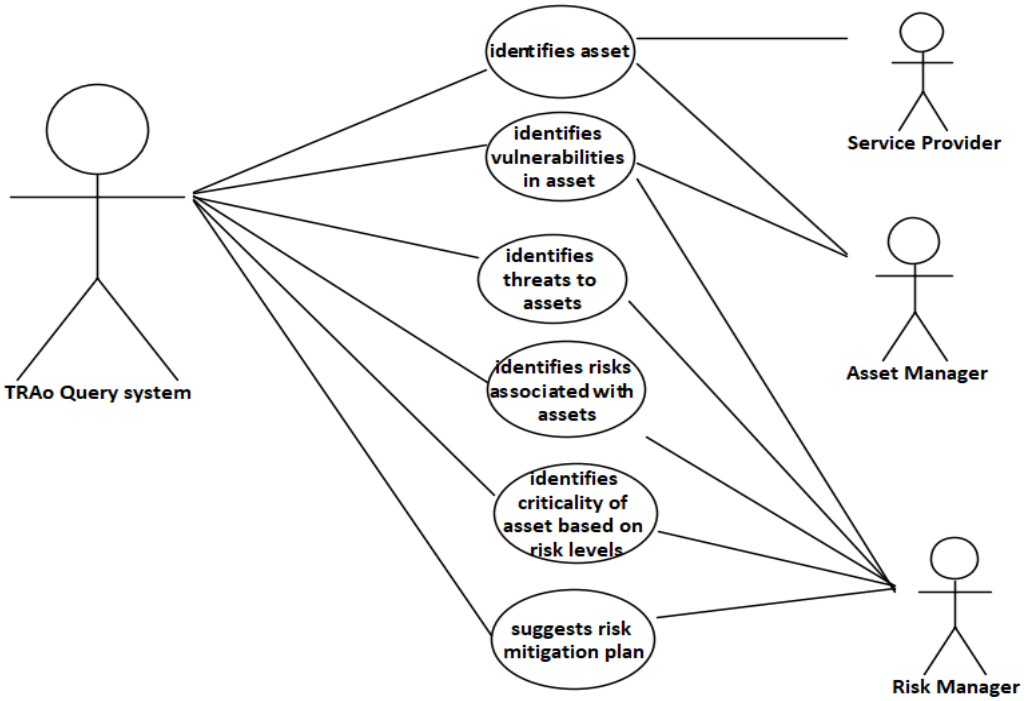


Figure 6. 21: Use Case Scenario for the Management of Risks

6.6 Design Process involved in the Analysis of Evolution-Related Risks

Based on the constructivist research method which was adopted as the research method in Section 5.3.4, the theory suggests that risks are only socially processed if they are cognitively constructed by social agents (Figueiredo et al. 2014). Thus, making many problems invisible. Furthermore, this thesis takes a fundamental part of its bearing in intelligence analysis which is increasingly being driven by the need for intelligence in ways that are unpredictable which require special expertise and the performance of core intelligence functions (Lillbacka 2013).

Systems in government must evolve while responding to a myriad of changes in government. Therefore, the E-Government system must be designed to cope with a number of security issues associated with evolving systems or components. The issue of making theoretical assumptions on which the design of a system is based should be avoided. Garlan et al. (1995) posits that architectural mismatches are a major universal source of problems and are a direct

result of assumptions that are mismatched. Another cause for failures in systems which is a risk is when invalid assumptions about operations in the real world are made by designers (Lipson 2006).

Thus, this thesis takes the stance of Lipson (2006) in designing the system for analysing evolution-related risks. It posits that:

"in the absence of countermeasures, a system's security and survivability will degrade over time. Changes in the environment or usage of a system, or changes to the elements that compose the system, often introduce new or elevated threats that the system was not designed to handle and is ill-prepared to defend itself against. The first step in evolving to meet new threats to your system's security and survivability is to recognize the need to modify your system — that is, to recognize changes in security and survivability risks that trigger the need to enter the evolution phase of the system development life cycle".

It is therefore essential to devote significant risk management resources to the ongoing evolution of any mission critical system and its associated processes. Again, this highlights the importance of intelligence analysis which the use of an ontology will provide. An ontology has predictive and detective capabilities given that it may be able to detect the changes that may affect assets. The assumptions made by an ontology through the inference engine will help in detecting changes that may affect assets on which the security of the system is founded.

6.7 Conclusion

This chapter has presented a conceptual framework for the key concepts in this research. The framework has presented descriptions on a key aspect that may be affected by evolution - interoperability. The different types of relationships surrounding interoperability have been presented which gives the reader an understanding of the effects this may have if there are risks that occur. This framework has also established that an asset may interact with a risk in a variety of ways which may also be based on the composition of an asset. An overview of the operations of this framework is presented which shows how EGov Services may be requested and the different processes involved in that. Enmeshed in the processes involved in delivering and providing a service are inherent risks. This is explained in further detail with the interpretive case study provided in Chapter 7. Furthermore, this chapter has been able to further answer RQ1, RQ2 and RQ3.

Chapter 7: Ontology Development and Hypothetical Scenario Modelling

The preceding chapters establish the need for the development of an ontology for managing the risks associated with evolution in E-Government. This chapter outlines the design of the ontology. With the use of hypothetical scenarios to aid the development of the ontology, this thesis shows how the integration of the core ontology modules can lead to improved management of assets while creating associated risk-awareness especially around managing the complex relationships that exist given the rate at which evolution occurs.

7.1 Design of the Threat Risk Asset Ontology (TRAO)

The design of TRAO involved building a knowledge base for the ontology. This knowledge base consisted of the development of an Upper Level ontology which was developed to represent the domain and application area; the domain specific-ontology which was developed to represent conceptualisations relevant to evolving risks in the E-Government domain and the scenario ontology which was used to model the specific scenarios that can be answered by the Domain and Upper level ontologies. The development of a domain ontology has advantages rooted in its ability to define the associated domain knowledge combined with a semantic model (Munir and Anjum, 2018).

At the time of developing TRAO, no standard ontology exists that models the relationships that exists between the different domains as well as models the risks associated with evolution in E-Government. There is also a lack of a single domain E-Government ontology that provides sufficient coverage for evolution related-risks with assets in E-Government.

7.2 Creating an Ontology Model for E-Government

Knowledge in domains are represented and stored when ontology-based models exist (Lim & Ko 2009). The development of the E-Government ontology followed a structured and systematic approach discussed in 5.7.5 and involved the use of the following steps:

1. Determination of the Domain, Purpose and Scope of the ontology: Considering the complexity of government, there is the tendency to include irrelevant pieces of data. However, laying out a scope made it possible to focus on the definition of data relevant to the E-Government domain, the users of the system as well as the risks associated with

evolution within the E-Government domain. The main goal of this step is to determine the main reasons and basis for the development of the ontology, the coverage of the ontology and the foreseeable granularity. This step also involved determining which language was the best fit for the development of the ontology.
The definition of the scope and boundaries of the ontology were carried out using several interviews with key stakeholders.

Furthermore, the determination of the purpose and scope of the ontology involved outlining the domain coverage, the use of the ontology, the type of questions to be answered by the ontology and whether the development of subontologies would aid the understanding of the ontology.
In line with outlining the purpose and scope of the ontology, the purpose of the development of TRAO is presented.

Threat Risk Asset Ontology (TRAO) is an ontology developed for the E-Government domain to understand the Threats and Risks associated with evolution in the E-Government domain. It is intended that changes associated with evolving EGov Services and assets will be managed with the use of this ontology and that the level of granularity is directly related to the competency questions. Due to the complexity associated with the subject, the ontology involves the development of several subontologies (EGov Service, IT_Asset, Threats, Risks etc).

2. **Identification of intended users of the ontology:** This stage involved identifying the users of the ontology. Considering that interviews were conducted with stakeholders to determine the purpose and scope of the ontology, this helped in narrowing the ontological needs of the users. The intended End users of the ontology are shown in table 7.1.

Table 7. 1: Intended End-users

End user	Description
1	SPs who are interested in understanding the risks of EGov Service evolution
2	Asset Manager who needs to know what assets are affected by evolving E Gov Service
3	Risk managers who must feedback to government officials the impact of certain risks

End user	Description
4	Third-Party providers who offer Third-Party services to government who must analyse the sustainability of their services E.g. Centre for protection of National Infrastructure.
5	Central and Local government who need to analyse the effect of evolution on government and who need to prepare policy documents.
6	Statisticians and analysts who must be able to analyse the effects of the steps taken towards evolution E.g. performance analysts, data scientists, data engineers etc.
7	Mergers and acquisition dealers' who must review such deals and laws in government as it relates to merging certain SPs or EGov Services E.g. Dept. of Justice, Office for National Statistics, Competition and Markets Authority etc.
8	Vendors/ Suppliers/Sub-system vendors, contractors, sub-contractors responsible for providing software, hardware, firmware and/or documentation to the organisation for a fee or in exchange for service. They must be able to consider security related-risks that may stand in the way of the services they provide.
9	Audit trailer who will need to manage and check inventories to make sure that documented system of recording are followed e.g. Audit Trailing Analysis Service (ATAS)[81] which is used by business systems in the UK such as the Department of work and Pensions.
10	Remote Support Staff who ensure that remote services and assets are used properly[82].
11	Government key stakeholders interested in predicting effects of change and evolution E.g. Cabinet Office, Government Digital Service (GDS)[83].
12	Government Transformation Strategists who are committed to the delivery of brilliant public services E.g. Cabinet Office, Government Digital Service (GDS)[84].

[81] https://data.gov.uk/dataset/58037850-9ef5-48e6-8e42-d91e90afa022/audit-trail-analysis-service-2
[82] https://data.gov.uk/dataset/7d950b30-72c7-475b-9584-0efe8fae37f6/ethos-remote-access-service-ras-user-database
[83] https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy
[84] https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy-tools-processes-and-governance

End user	Description
13	Data analysts who are interested in providing consistent and homogenous data from heterogenous data sources[85]

3. Reuse of Existing Ontologies: Existing ontologies were considered for reuse during the development of the ontology. The reason for this is to identify possible ways by which existing ontologies relating to the domain of discourse could be extended or re-engineered. There was no suitable ontology that could be directly reused, therefore subontologies were identified. Ontologies which were identified for reuse include the following:

a. Security ontology (Fenz, 2010) which was used to model the relationships that exist between assets, threats and vulnerabilities. This ontology was based on the model described by the National Institute of Standards and Technology (NIST, 1995).

b. Ontology of information security (Herzog, Shahmehri and Duma, 2007): This ontology describes security technologies as a taxonomy and defines classes that sort assets based on their corresponding countermeasures and threats, security goals and defence strategies. This ontology was used to build the high level of the corresponding classes in TRAO.

c. Inspire Ontology (Bouet and Israel, 2011): This ontology was used to model complex relationships in the form of interdependencies that exist between critical infrastructures.

d. Ontology for Vulnerability Management (OVM) (J. Wang et al. 2010): This ontology was used to model vulnerabilities that may exist in an asset.

4. Scenario Formulation: The use of scenarios in this ontology model how a task or query can be achieved based on a sequence of interactions with the system. Different scenarios that were plainly written in English and not logic-based were produced and were answered using plain English too. These scenarios are presented in Sections 7.4, 7.5 and 7.6. As a way of defining the scenarios and communicating them to the right people the scenarios are developed in the form of stories and they include possible solutions to the problems. Ideally the scenarios were developed for the intended kind of use for this ontology by envisaging the different kind of questions that may come up during its use. Their development at the

[85] https://data.gov.uk/about

beginning of the research necessitated the need for them to undergo refinement during the research. The development of the scenarios was compiled from a variety of sources and it involved the development of two types of scenarios namely High-level scenarios and detailed user scenarios. The high-level scenarios were formulated because of their importance in defining and understanding the broad scope of the research while the detailed user scenarios were used to drive the development of specific features of the ontology. The formulation of scenarios for this research have been mostly hypothetical and are used solely for illustration.

5. Competency Question (CQ) Formulation: A natural language sentence that expresses a pattern for the type of questions people expect an ontology to answer is called a Competency Question (Uschold and Gruninger, 1996). CQs written in natural language were formulated to represent the requirements of the ontology. The CQs for the ontology were developed hierarchically starting with general ones and then narrowing it down to specific ones. This was in accordance with the CQs approach presented by Uschold & Gruninger (1996).

The adequacy of TRAO is tested with the development of a set of CQs. Some of the CQs addressed and used to evaluate TRAO are presented in Table 7.2.

Table 7. 2: Sample List of Competency Questions

CQ	**Asset-related competency questions**
CQ1	Who owns an asset?
CQ2	What assets does an EGov Service service require to run on?
CQ3	What are the risks associated with each asset?
CQ4	What vulnerabilities is an asset vulnerable to?
CQ5	What is the impact of a particular risk occurring?
CQ6	What types of relationships exist between assets?

CQ	Asset-related competency questions
CQ7	What are the components of an asset?
CQ8	What is a single asset?
CQ9	What is a complex asset?
CQ10	What is a reusable asset?
CQ11	What is a dependent asset?
CQ12	What is an interdependent Asset?

CQ	Risk-related competency questions
CQ1	What are the risks associated with dependencies of single/complex systems, components or infrastructures?
CQ2	What ways can the risks associated with single/complex systems be analysed?
CQ3	What are the types of evolution-related risks that occur as services evolve?
CQ4	What kind of risks can reuse of assets introduce?
CQ5	What impact does an evolving service or asset have on other services or assets?
CQ6	What kind of risks occur if a service or system is decommissioned?
CQ7	What are the types of evolution-related risks that occur as services evolve?
CQ8	What are the risks associated with dependencies of multiple dependent assets?
CQ9	What is the likelihood of a risk occurring?
CQ10	What is the cause of the risk?

CQ	Risk-related competency questions
CQ11	How serious can the consequences of this risk be for the service providing organization if this risk occurs?
CQ12	What assets are affected by a particular risk?
CQ13	How many high risks have been identified?

6. Development of Templates for ontology: The complexity of the E-Government domain motivated the development of scenario templates so that domain knowledge can be properly organized and utilized. Also, the use of templates allows for reusability since they can be reused across multiple scenarios. An example of a template for finding out about Assets and corresponding Asset components is presented in table 7.3.

Table 7. 3: Sample Template for Asset and Asset Components

isPartOfAsset(Asset_Component,Asset) :: {Asset v ∃hasPart.Asset_Component} is the template isPartOfAsset which has a single axiom knowledge base { Asset v ∃hasPart.Asset_Component } where hasPart is a relationship between Asset_Component and Asset are the classes. isPartOfAsset(Virtual_Machine, Operating_System) are instances of PartOfAsset represented in the ontology.

7.3 Building in Natural Language into the Ontology

Natural language generation is a task associated with the generation of human understandable text. It involves representing facts in machine language in a form that is linguistically acceptable (McCoy 2012). Ontologies are based on natural languages and are structured like systems in which the primary and principle node is the word which is converted to a term (Curras 2013). The formal structure of an ontology does not allow for easy interaction for those who do not have any knowledge of ontologies. It is considered as a repository which serves as a resource for natural language tasks (McCoy 2012). While a domain ontology is used for content determination of the ontology, a linguistic ontology would be used for lexical realisation.

Ontologies represent real world knowledge, but this representation is in form of concepts,

individuals and relations in Description Logic. Since ontologies contain knowledge they can be likened to repositories of knowledge and can serve as inputs to Natural Language Generation (Gyawali 2011). They are a core technology for the development of high-quality knowledge-based systems that are effective (Fensel 2004). Interactions with the ontology are carried out based on Question-Answering system. A Question and Answering system was defined by (Davies et al. 2006) as "*an information retrieval application whose aim is to provide inexperienced users with flexible access to information, allowing them to write a query in natural language and obtaining not a set of documents that contain the answer, but the concise answer itself".* The queries are put in by the user in natural language which will be used as the determiner of the content for Natural Language Generation. The output received as an answer to the user query is received in natural language (McCoy 2012).
The reason we need to build in natural language to interface with TRAO is because of the kind of questions a human may ask. Typical examples of a question a user may ask with respect to this ontology in the E-Government domain are:

What Assets are exposed to a technical risk?

7.4 Development of the TRAO Framework

The TRAO framework is composed of three overarching core components – EGov module, The Asset Module and the Security module. The EGov component aggregates information relating to Stakeholders, EGov Services, IT Services; the Security component aggregates vulnerabilities, threats, risks, safeguards from various sources and consolidates them into a centralised place. The Asset module aggregates information related to IT assets. However, each ontology module has an associated module known as the Specialised view {Asset_Specialised_View, Threat_Specialised_View, Risk_Specialised_View etc.}. These views were created to model the specific scenarios of the ontology referred to in the diagram as the Scenario recommender.

Figure 7.1 presents a diagram of the ontology framework developed in relation to this study. It is developed as a functional architecture consisting of three layers. The first layer is referred to as the layer where specific ontology querying takes place. The second layer consists of the TRAO recommender systems which offer relevant information on different key aspects relating to the various subdomains. The middleware infrastructure consists of the TRAO rule engine which contains Semantic Web Rules defined in the ontology while

the semantic matching engine enables semantic web capabilities for the recommender systems. The third layer consists of the ontology modules developed for TRAO.

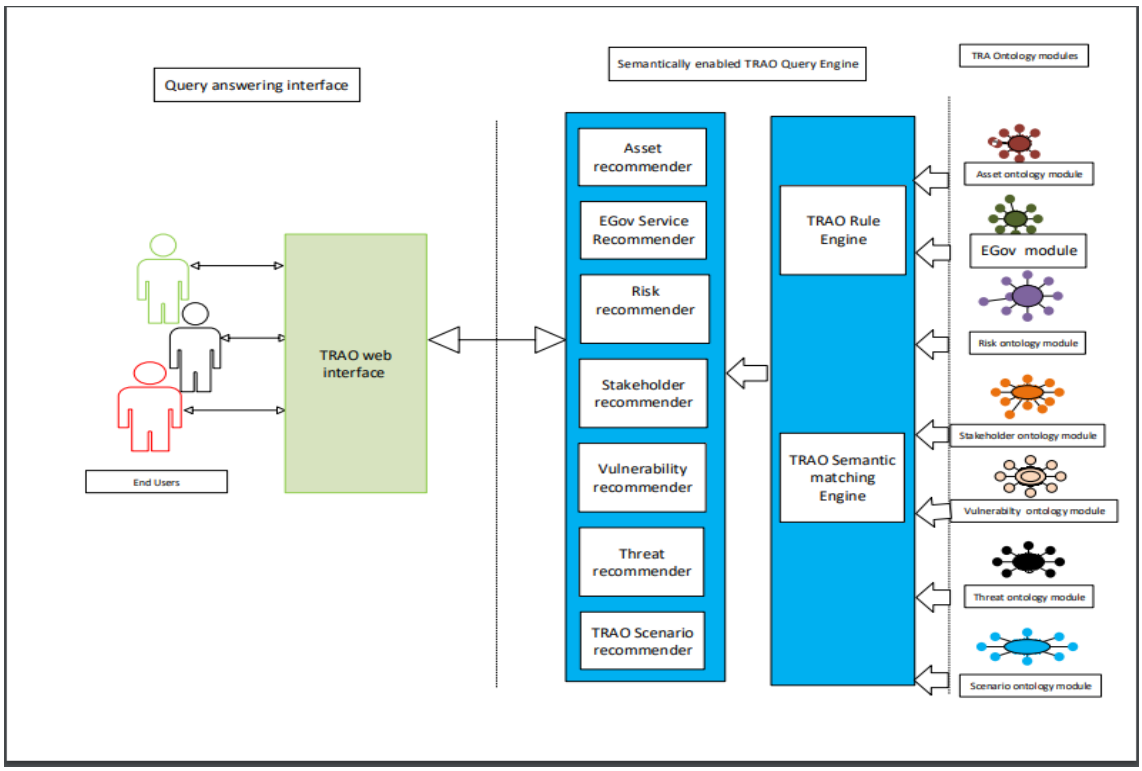


Figure 7. 1: The TRAO Framework

7.5 Development of Generic Modules within the Ontology

The design and development of the ontology was based on the outputs from the requirements of the ontology obtained from the development of the competency questions. Considering that an ontology is any specification of a conceptualisation, they can include any kind of representation or model. This may involve the development of taxonomies, flow-charts, entity relationship diagrams etc. This research involves the use of the Semantic Web Ontology Language (OWL) and its automated reasoning functionalities to adequately describe E-Government ontologies because it is one of the most well-developed languages for building ontologies. The objectives behind the development of the comprehensive ontology include the following:

1. To develop an intelligent tool that uses an ontology describing E-Government, EGov Services, IT Services, Stakeholders, Assets, Security (Covering Risks, Vulnerabilities and Threats);

2. To enable stakeholders', identify what EGov Services pose a risk based on the IT Services and Assets that they make use of. This is achieved by the construction of queries against the ontology with the use of the tool and obtaining results that are reasonable without dealing with underlying representations or the concrete syntax of the ontology.

The TRAO has been developed as a sufficiently decidable and expressive ontology given that finesses and important details of the ontology are covered in its vocabulary. The capabilities of a reasoner allow new facts about axioms and constraints within the ontology to be inferred thus enriching the conceptual schema.

7.5.1 Developing the E-Government Module of TRAO

In developing the E-Government module, the WSMO-PA model which modelled the activities performed in public administrations was used. However, this model was extended to incorporate major stakeholders and EGov Services.

Figure 7.2 presents a diagram on the different classes of Stakeholders that exist in E-Government in relation to the defined domain.

Stakeholder ∋ Service_Receiver ∧ Asset_Manager ∧ Asset_Owner ∧ Risk_Owner ∧ EGov_Service_Provider ∧ IT_Service_Provider

Service Receiver ∋ Citizen ∧ Business ∧ Government

EGov_Service_Provider ∋ Ministry ∧ Department ∧ Backup_Service_Provider ∧ Critical_Service_Provider ∧ Supporting_Service_Provider ∧ Agency ∧ Dependent_Service_Provider ∧ Third_Party_Service_Provider

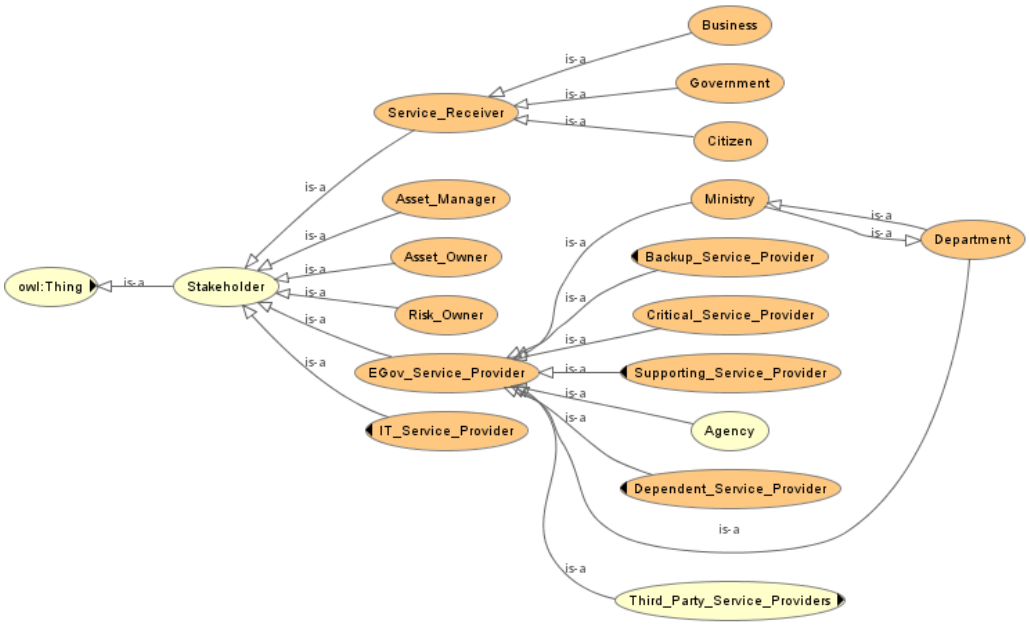


Figure 7. 2: Modelling of Ontology to Show the Different Stakeholders in the Ontology

Figure 7.3 focusses on the SR Stakeholder with a modelling of the subclasses of the SR class in the form of Government, Citizens and Businesses. This modelling was developed in order to map the SRs to the class of Events which models the Life event, Government Event and Business Event classes. The relationship that exists between the SR class and the EGov Service class is defined with the *receivesService* relationship. Figure 7.4 presents a diagram that shows the relationship a SP has with an EGov Service. This relationship is defined with the *providesSevice* relationship

The ***receivesEGovService*** property relates a Service_Receiver instance that ***receivesEGovService*** instance to the EGov_Service.

```
EGov_Service:receivesEGovService a owl:ObjectProperty ;
                rdfs:label "consumes"@en ;
          rdfs:domain service:Service_Receiver ;
          rdfs:range EGov_Service:EGov_Service ;
        owl:inverseOf EGov_Service:isReceivedBy ;
                rdfs:isDefinedBy <> .
```

Service Receiver {Business, Citizen, Government} *receivesEGovService* {G2B_Service, G2C_Service and G2G_Service}.

Similarly, EGov_Service {G2B_Service, G2C_Service and G2G_Service} *isReceivedBy* Service_Receiver {Business, Citizen, Government}

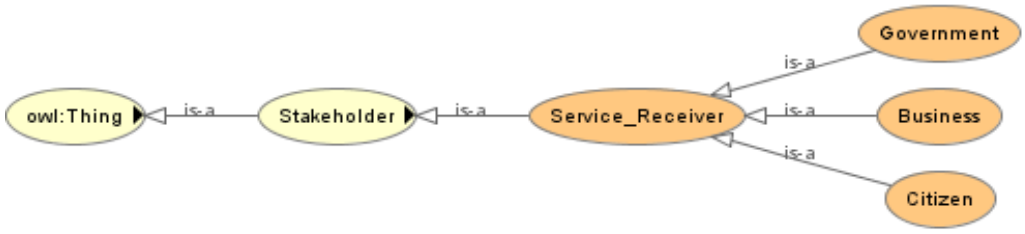


Figure 7. 3: Modelling of Ontology to Show Relationship between SRs using OWLViz

The ***providesEGovService*** Relates an EGov_Service_Provider instance that ***providesEGov_Service*** instance to the EGov_Service.

```
EGov_Service:providesEGov_Service owl:ObjectProperty ;
rdfs:label "providesEGovService"@en ;
rdfs:domain EGov_Service:EGov_Service_Provider ;
rdfs:range EGov_Service:EGov_Service ;
owl:inverseOf EGov_Service:isProvidedBy ;
rdfs:isDefinedBy <> .
```

EGov_Service_Provider subclass Department *providesEGovService* EGov_Service Department has instances of GovernmentDigitalServices, DeptOfEducation, DeptOfTransport …..

The ***isProvidedBy*** property relates an EGov_Service instance that ***isProvidedBy*** **an EGov**ServiceProvider instance to the EGovServiceProvider.

```
EGov_Service:isProvidedBy a owl:ObjectProperty ;
rdfs:label "isProvidedBy"@en ;
rdfs:domain EGovService:EGov_Service ;
rdfs:range EGov__Service:EGov_Service_Provider ;
owl:inverseOf EGov_Service:providesEGovService ;
rdfs:isDefinedBy <> .
```

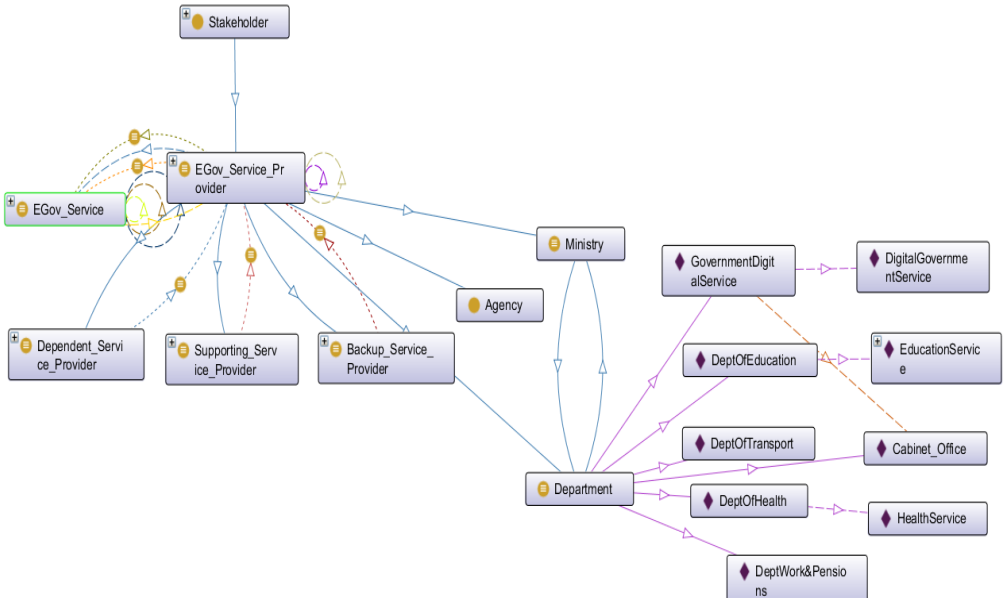


Figure 7. 4: Modelling of Ontology to show the Relationship between SP and EGov Service

7.5.2 Modelling the Relationships between IT Services and EGov Services

The operations of most organisations are driven by the operations of their IT infrastructures. Thus, a change in the processes within an organisation bring about a change in the IT

infrastructure (Brocke et al. 2013). In Section 3.3, it was established that EGov Services require IT Services for their operation. An EGov Service may require the operation of at least 1 IT Service. Thus, resulting in complexity in the E-Government domain considering that IT Services make use of Assets to make the EGov Services available. Identifying the relationships that exist between IT Services, EGov Services and the assets they make use of is necessary.

IT governance framework is another body of knowledge on which the artefact of this research is grounded in. It has a direct impact on how organisations manage IT (Sohal & Fitzpatrick 2002). Existing taxonomies grounded in widely accepted IT governance frameworks (ITIL v3 and COBIT v5) were used. These were used because they are a collection of best practices and standards that encompass a vast amount of IT management knowledge.

The IT Service class models the three (3) types of ITIL Services. These are modelled as subclasses in the ontology which are: Core_Service, Supporting_Service and Enhancing_Service and this is represented in Figure 7.5.

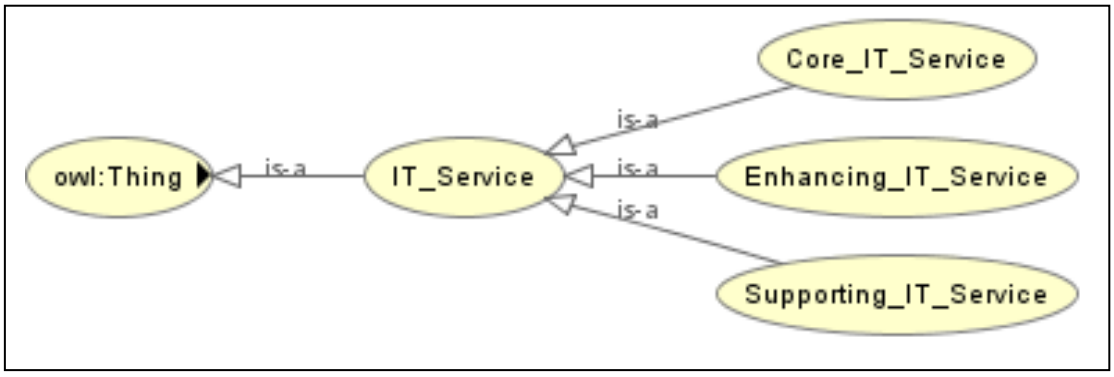


Figure 7. 5: Modelling of Ontology to show IT_Service using Ontograph

As an example, based on the modelling of the ontology

Supporting/Core IT Service (ITS1, ITS2): {ITS1} *enablesCoreService* {ITS2}. Thus, {ITS1} is the Supporting_Service of {ITS2} and {ITS2} is the Core_Service of {ITS1}. This means that {ITS2}is the main service required to provide an EGov_Service while {ITS1} is not required to initiate the EGov_Service that {ITS2} initiates. Therefore, {ITS2} cannot be provisioned without {ITS1}.

Enhancing/Core IT service (ITS1, ITS2): {ITS2} is an enhancing service of {ITS1} (and thus {ITS1} is a core service of {ITS2}. Therefore, the modelling of the ontology shows that

an enhancing service like {ITS1} is an optional service element next to {ITS2} and is not necessarily required for the provisioning of service {ITS1}.

To represent the relationship that exists between and EGov Service, an IT Service and an IT_Asset; an EGov Service is defined as one that requires an IT Service where the IT Service also requires an IT Asset. Invariably an E_Gov Service requires an IT_Asset

7.5.3 Development of the Asset Module

In developing the asset module of the ontology, professional knowledge of asset is built into the asset module according to OWL, RDF and semantic web techniques. In doing this, an asset is assigned a specific state. In the report produced by the Department for Victorian Communities they state that there is the need for procedures that would help in acquiring, operating, maintaining, renewing and disposing assets (Department for Victorian Communities 2004). Appropriate systems are needed to capture and record information about each asset and this is where the use of an ontology plays a vital role. The use of an ontology would support the identification of an asset, the value of the asset, its condition, decommissioning date and even provide useful information to support other systems connected to it. This section discusses the various areas that were focussed on while modelling the asset ontology module.

Asset registers have been known to be created and maintained manually by recording basic details of assets or sometimes the use of asset management software is employed. The use of an ontology has the potential of identifying, recording and recognising assets as well as the relationship that a particular asset has with other assets. Ontologies help to manage restrictions that may be placed on assets as a restricted asset would not be made readily available. They also help to give privileged access to a particular SP despite the links and relationships an asset may have with other assets in terms of being shared across SPs.

Describing the properties of assets is a crucial first step towards developing a prototype tool to run queries. However, capturing the relationships that exist between assets is very challenging because of the existence of seemingly disconnected sources of assets in varying formats. Thus, semantic metadata of assets must be captured so that issues of integrations can be addressed. For example, it is unrealistic, and contrary to practice, to assume that all asset managers shall refer to assets using the same name.

The asset module of TRAO is implemented using two types of OWL properties namely object properties and data properties. Object properties such as: *backsUpAsset, dependsOnAsset, hasPart, hasRelationshipValue, hasState, assetHasVulnerability, assetIsInterdependentOn, isExposedToRisk, isReusedBy etc.* are defined as the subclass of OWL owl:objectProperty and are used for linking the Asset class to other classes. The datatype properties such as: *Asset_ID, Asset_Name, Asset_Location, Asset_Decomission_Date etc.* are defined so that the built-in OWL owl:DataType property can be extended for assigning plain/literal string values to the properties of assets. Thus, complex data relating to assets can be represented in highly accurate formats because this enables syntactic homogeneity across the ontology using RDF/OWL constructs. Table 7.4 presents the data properties that are defined in the ontology in relation to an asset.

Table 7. 4: A Conceptual Schema for Representing Asset Data Properties

PROPERTY NAME	DATA TYPE	DESCRIPTION
ASSET_ID	String	Unique Identifier of each Asset
ASSET_NAME	String	Asset name
SYNONYM	String	Other names used by professionals
ASSET_LOCATION	String	Location of each asset
ASSET_CREATION_DATE	DateTime	Date asset is created
ASSET_DECOMISSION DATE	DateTime	Date asset is decommissioned
AGE	integer	Age of the asset in years
VERSION	String	Version of an asset e.g. Windows 10

7.5.3.1 Modelling of the Asset Module of the Ontology

Figure 7.6 presents the high-level view of the modelling of assets in the ontology. There are different classes of assets that exist in the ontology which show the high-level assets which the ontology models. A class on Examples of assets shows low-level specific type of assets.

Figure 7. 6: Subset Overview of the IT_Asset Module of the Ontology

7.5.3.2 Modelling Generic Relationships between Asset and Asset Component

Figure 7.7 presents the components that make up An Asset. Each high-level asset as shown in Figure 7.6 has a corresponding asset component.

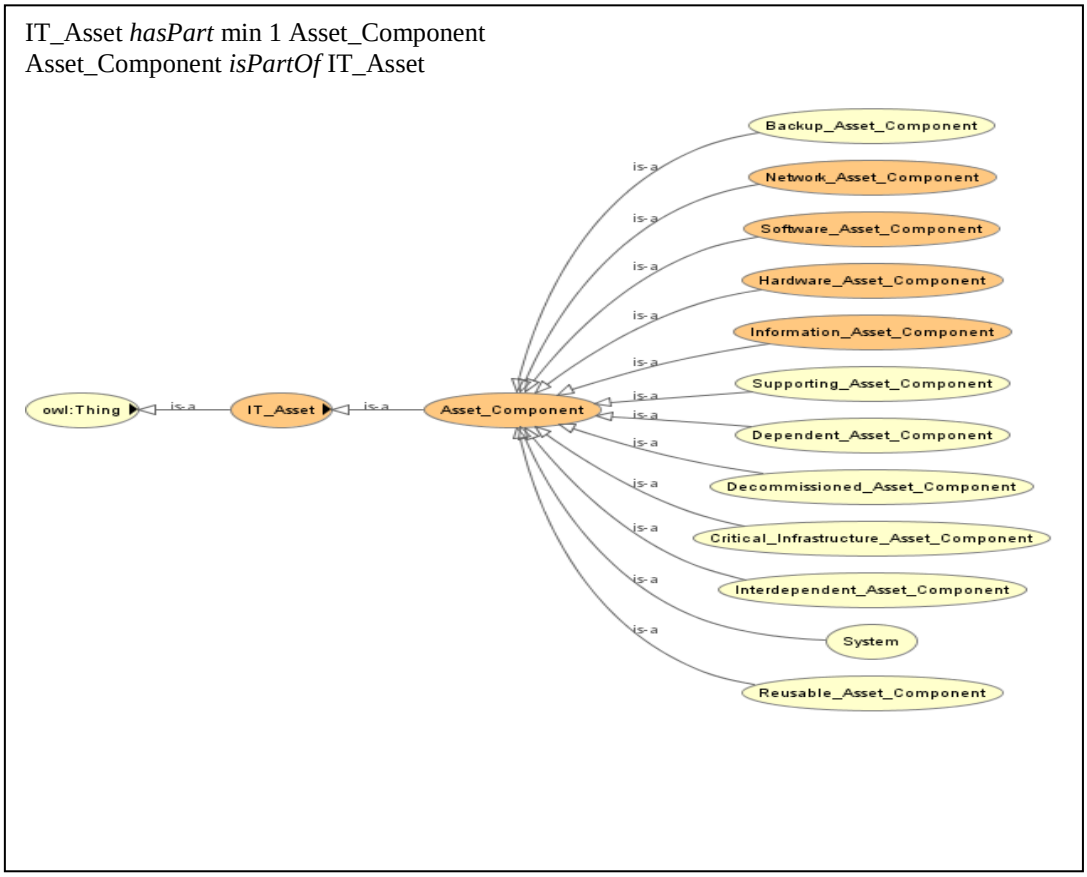


Figure 7. 7: Subset Overview of the Relationship between IT_Asset and Asset_Component

7.5.3.3 Development of the Asset Module – Identifying Reusable Assets

This involves identifying areas of reuse. This could be in the form of applications, equipment or resources that are reusable. To achieve this, a comprehensive cross-government asset register is populated. There is also the aspect of reuse of business applications and components across the public sector which is also modelled in the ontology. An ontology of reusable assets named ONTO-ResAsset was developed by (Da Silva et al. 2014) and was evaluated from the viewpoints of domain experts and non-experts. The knowledge obtained from the results of this research was applied in the development of the ontology considering that professional knowledge of assets managed and used by governments were built into this ontology. Knowledge about assets and their management are spread throughout various pieces of literature, books, as well as standards. This knowledge may not be readily

accessible because they exist in different formats as well as several levels of abstraction. The limitations of getting readily accessible information on assets and its management has led to the need for unification and organization of knowledge about assets. In his paper, Gruber (1993) proposed the use of ontologies in overcoming this limitation of conceptualizing knowledge.

Figure 7.8 shows the relationship that exists between an asset (Reusable Asset), risk (Reusable Asset Risk), asset component (Reusable Asset Component) and the Stakeholder responsible for reusing an asset.

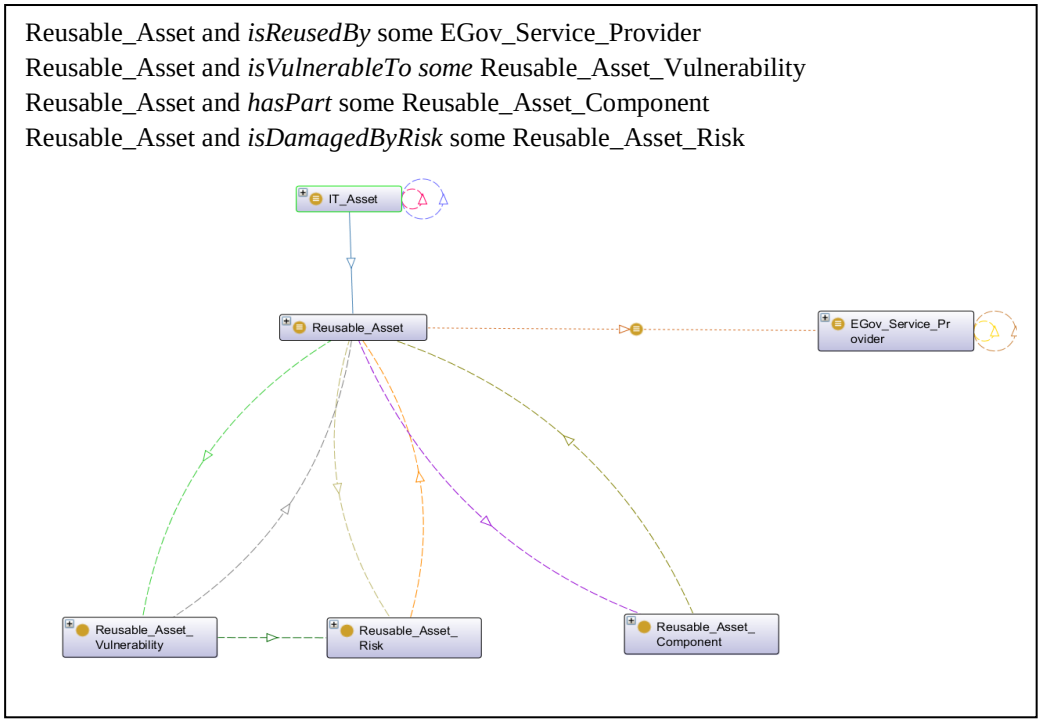


Figure 7. 8: Generic Modelling to show the Relationship of Reusable Assets

7.5.3.4 Development of Asset Module - A focus on Critical Assets

Every asset carries with it the risk of failure. However, there is a variance in the failure risk each asset presents. Similarly, not every asset is critical to the operation of infrastructure that are critical. The importance of knowing which assets are critical and the ones that are required to sustain critical operations of a system is invaluable. Critical assets can be seen as those assets that present a greater risk of failing and have major impacts if they fail. Ranking assets based on their level of criticality in the domain which they are being described in is of great use especially as a proactive solution in planning and finding other assets that may be used on an ad hoc basis.

The modelling of critical infrastructures is done at two levels in the ontology which are at the single system level and at the level at which systems are composed of other systems commonly referred to as the system-of-systems level. Understanding the reasons for the existence of relationships (dependence and interdependence) between Critical Infrastructures and the risks associated with these relationships are important. The understanding that Critical Infrastructures are critical to the running of certain EGov Services within E-Government is important and questions would need to be asked to support their existence:

What critical assets are prone to failure?
What is this Critical infrastructure (CI_1) *dependent on?*

What ad hoc assets are in place?
Is a Critical Infrastructure able to adapt to change if failure occurs?

On attempting to answer these questions and model them into the ontology, the following best practices were also employed.

1. Assets were assigned unique IDs: Crothers (2009) insists that it is an absolute must to use unique asset IDs. He believes that unique asset IDs play a critical role in reducing information about assets that is duplicated or confusing and that the assignment of unique IDs is the first step to reducing data silos as well as increase the integration of systems. In the development of the ontology, assets had to be defined in terms of criticality. The higher the criticality of an asset, the greater the impacts of the risk associated with it. What assets are defined as critical?

2. Assets were modelled into the ontology in terms of level of criticality. So, each asset is assigned a critical number in terms of criticality ranging from 1-10. Assigning a critical number to an asset is different from the asset ID no. For Example, Asset A1 can have a critical number of 1 and have an asset ID of 001. Assigning critical ratings to a number provides a method for prioritization especially with respect to risks.

Table 7.5 describes the values used to model asset criticality ratings in the ontology. These values were defined both quantitatively and qualitatively.

Table 7. 5: Asset Value Scale (Adapted from FEMA)

Asset value	Numerical Value
Very Low	1
Low	2-3
Medium Low	4
Medium	5-6
Medium High	7
High	8-9
Very High	10

3. Assets were also modelled based on the likelihood of probability of failures. This assumes that all assets have a probability of failure and it needs to be determined whether age, usage or condition of an asset can be substituted for another asset. Table 7.6 describes the values used in the ontology to model the probability of failure based on the percentage of effective life consumed. This was modelled so that it could be determined whether an asset was still valuable for use.

Table 7. 6: Linking Probability of Failure to Age of Asset (percentage effective life consumed)

% of Effective Life Consumed	Percentage of Failure Rating
<10	1
20	2
30	3
40	4
50	5
60	6
70	7

% of Effective Life Consumed	Percentage of Failure Rating
80	8
90	9
Failed	10

4. Assets were also linked to direct observation based on probability of failure.

Table 7. 7: Linking Probability of Failure to Direct Observation Tables

Asset Assessment	Probability of Failure weighting	Failure Description
Very Low	1	Expected to occur within 100 years
Low	2	Expected to occur within 50 years
Moderate	10	Expected to occur within 10 years Estimated 10% chance of occurring in any year
Quite Likely	20	Expected to occur within 5 years Estimated 20% chance of occurring in any year
High	50	Estimated 50% chance of occurring in any year
Very High	75	Likely to occur within a year
Almost certain	100	Expected to occur within a year

7.5.3.5 Development of the Asset Module – Identifying Interactions between IT Infrastructure and Assets

In their paper, a situation is described by Aime & Guasconi (2010) where the assessment of a risk to the IT infrastructure is dependent on the interactions they have with other assets. It is also possible to have specialised overviews about how systems within government are configured. A visual representation between systems and infrastructures within government is a good step in analysing the structure of government networks. Figure 7.9 shows an example of the relationship an asset has with other assets.

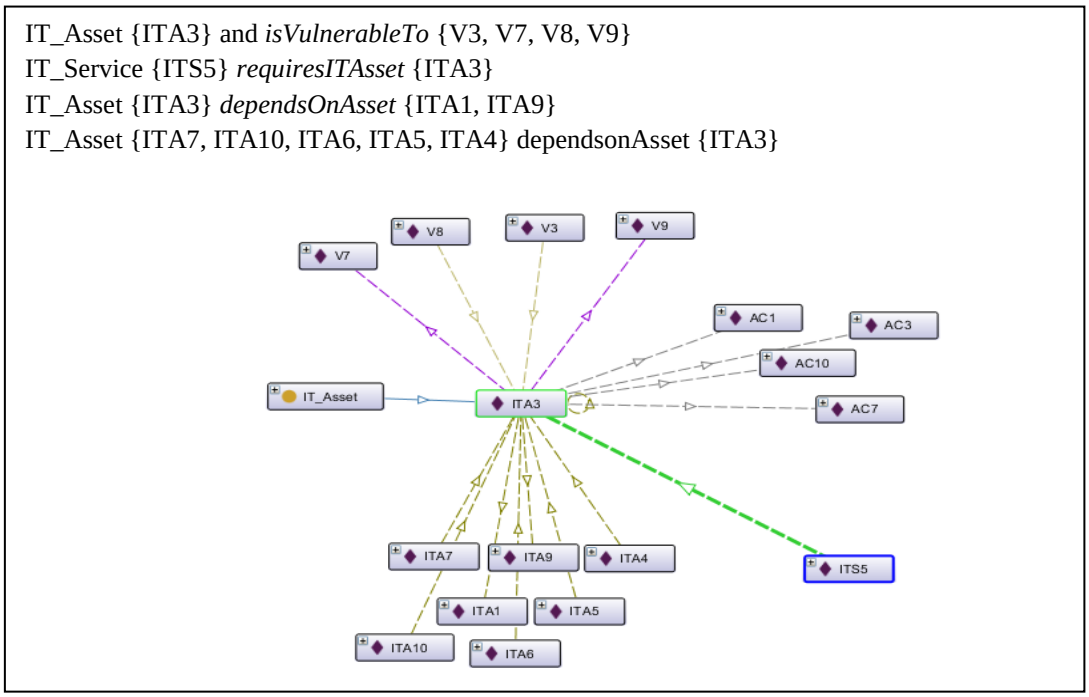


Figure 7.9: An instance of an IT_Asset showing the relationship it has with other assets, asset components and IT_Services including the vulnerabilities associated with the asset

7.5.3.6 Expressing the State of an Asset with the Use of a Set of Individuals

To model the state of assets represented as Asset_State within the ontology, the ontology uses the functional property of hasState to show that an IT_Asset can only have 1 Asset_State.

This approach considers the enumeration of the individuals Active_State, Available_State, Decommissioned_State, Defective_State, Disposed_State, In_Maintenance_State, In_Use_State, Lost_State, Missing_State, Pending_Disposal_State, Pending_Install_State,

Pending_Repair_State, Pre_Allocated_State, Reserved_State, Retired_State, Stolen_State which belong to the class Asset_State.

The reason for including the states of an asset is so that risks can be associated with each state of an asset.

Interpreting that "PC1 is decommissioned", is to say that PC1 has the value Decommissioned_State for Asset_Status. Furthermore, each of these states are made different from each other with the differentFrom axiom so this means that no 2 states are the same. The inclusion of the differentFrom axiom is in accordance with OWL not being able to make the Unique Names Assumption. The modelling of Assets and Asset_States is shown in the class-instance diagram in Figure 7.10.

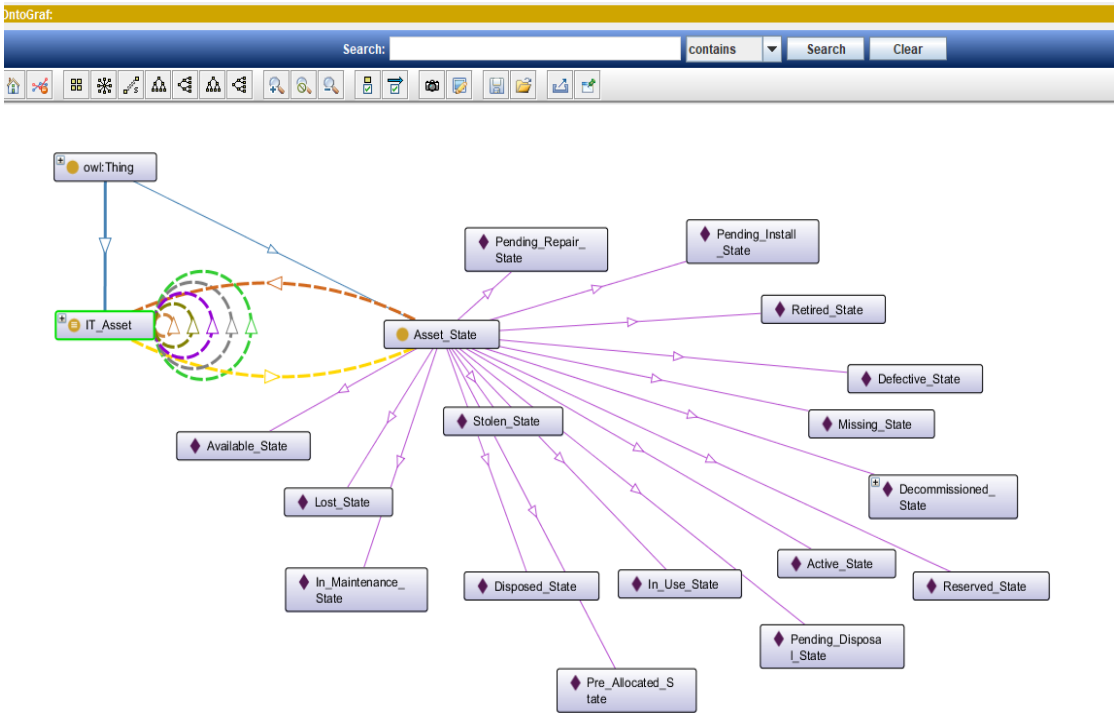


Figure 7. 10: Modelling of Ontology to Show the Different States an Asset can have

7.5.4 Developing the Security Module of the Ontology

Different ontologies exist in the security domain that already include some concepts for IT assets (Fenz & Ekelhart 2009; Tsoumas & Gritzalis 2006; J. Wang et al. 2010). In their paper, (Birkholz et al. 2012) stated that the concepts that represent assets often exist in the centre of the object property chain in previously developed security ontologies. They highlighted some notable examples to explain the link between assets and relationships as

well as security concepts such as the link between actual vulnerabilities to threats; the relationship between threats and impacts or even to security controls. An asset can have cascading relationships which may cause related assets to be compromised. It may also have cascading relationships which can be resolved by a single asset e.g. a local security control, countering a vulnerability associated with an asset. However, there are some that need information about the asset which could be as a result of a topological interconnection of assets, e.g. an external threat, exploiting a vulnerability associated with an asset (Birkholz et al. 2012). Our research is interested in the topological interconnection of assets within the E-Government domain and what threats can arise from this. We present this in our ontology as well as build on the work Aime & Guasconi (2010) in their research on Enhanced Vulnerability Ontology. They discussed the need for information about assets as well as their physical and logical interconnection topology. Considering the complexity of interconnected assets within a real system, (Birkholz et al. 2012) argue that it is important to acquire various configuration and neighbourhood information in detail because although representation of interconnected relationships between assets is essential, it is seen as quite abstract. The Interconnected Asset Ontology framework was developed by Birkholz et al with a strong focus on automatically acquiring information on assets with a high level of detail (Birkholz et al. 2012). A strong point of their proposed framework is that the equivalent level of detail is preserved in the ontological representation. Syalim et al. (2009) disclosed that carrying out major risk analysis is dependent on the asset information that is available. Their analysis is in agreement with (Birkholz et al. 2012) but is different in the sense that they stress that "*IT asset information is crucial for the assessment of potential threats and impacts (magnitude of harm) associated with a threats exercise of a vulnerable IT asset*" (Syalim et al. 2009). The work done by Singhal & Singapogu (2012) is relevant to this study because it involved the development of an ontology focussed on identifying threats that endanger assets and the countermeasures which can be put in place to reduce the probability of a damage occurring. Figure 7.11 presents the overall view of the security module used in the development of the ontology. This module focussed on building upon the components of risk analysis proposed by Whitman & Mattord (2014) which include assets, threats, countermeasures and vulnerabilities. Each of these components is refined with technical concepts. From Figure 7.11, the concept of vulnerability is connected to an asset with the *is-vulnerable-to* relation. A threat *threatens* an asset and a security mechanism/ countermeasure *protects* an asset. A security mechanism *satisfies* a security objective.

An asset is connected to the concept vulnerability through the *assetHasVulnerability*-relation or through the inverse relationship between Vulnerability and an asset with the *existsOnAsset* property. An asset *isThreatenedBy* threats that also denote which security goal they threaten. An asset is protected by countermeasures; a countermeasure is also an asset. A countermeasure protects a security goal and an asset with a defence strategy. For example: The countermeasure 'backup' protects the integrity and availability (security goals) of the asset 'data' through recovery (defence strategy). Instances of the concept defence strategy are prevention, detection, recovery, correction, deterrence and deflection. Instances of the concept security goal are confidentiality, integrity, availability, authentication, accountability, anonymity, authenticity, authorisation, correctness, identification, non-repudiation, policy compliance, privacy, secrecy and trust. Security goals may be related. For example, privacy has the related goals confidentiality, anonymity and secrecy.

7.5.4.1 Development of the Security module – Modelling the Relationship between Security and Assets

In this section, the reasons for introducing an asset module in the ontology are presented. This module consists of the different terms related to assets within a government and it is introduced into the ontology so that an overall assessment of risks relating to assets in a government is represented. This module also shows how risk management is incorporated with asset management within the ontology by representing the relationships that exist between risks and assets.

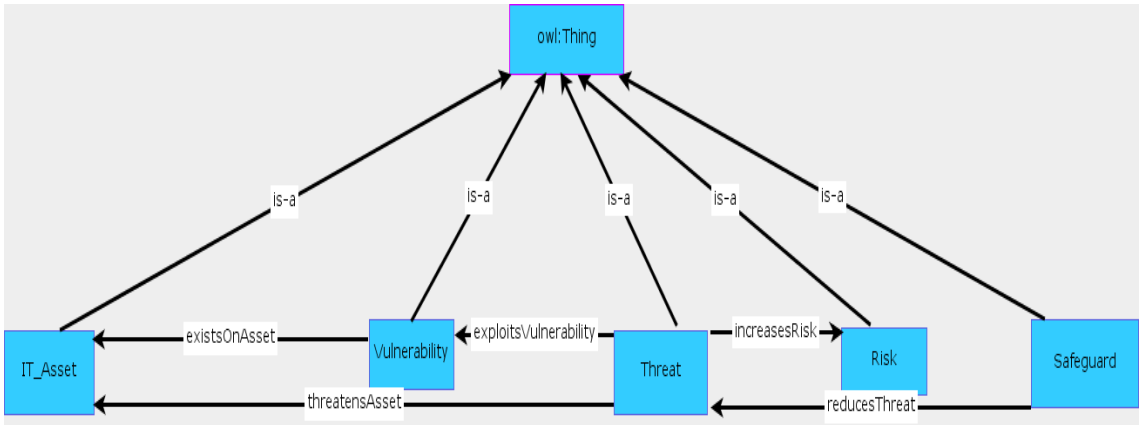


Figure 7. 11: Modelling of Ontology to show the Incorporation of Security Concepts

IT_Asset *isOwnedBy* some Service_Provider
IT_Asset *hasAssetVulnerability* some Vulnerability
IT_Asset *isThreatenedBy* some Threat
Threat *threatensAsset* some IT_Asset
Threat *increasesRisk* some Risk
Threat *givesRiseTo* some Threat

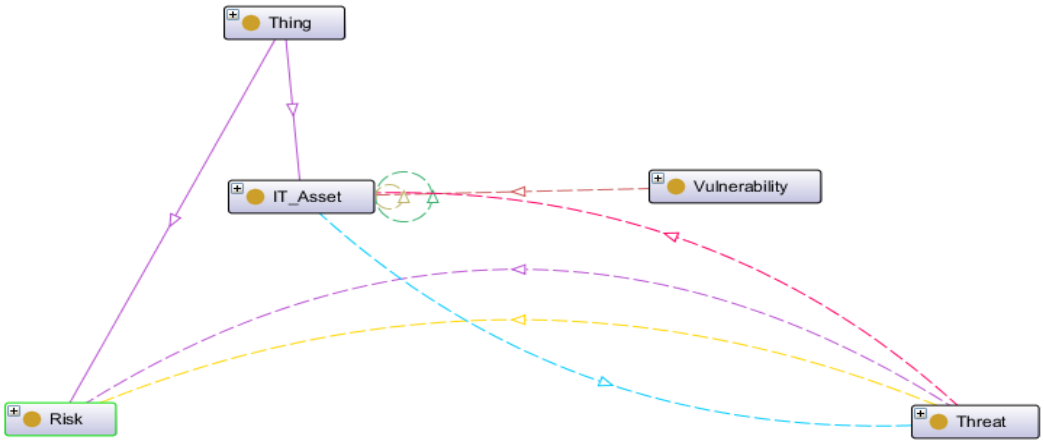


Figure 7. 12: Modelling the Relationship between IT_Asset, Vulnerability, Threat and Risk

7.5.4.2 Development of Security Module: Vulnerability Modelling within the Ontology

Although there are several technical white papers and work on vulnerability modelling, it has been impossible to locate any OWL files for Vulnerability Management. In developing the module of Vulnerabilities within the ontology, the method used by researchers in MITRE corporation is adopted (CAPEC, 2018).

This method assigns each vulnerability a unique identification number which makes tracking vulnerabilities easier. The module on vulnerability captures concepts and relations that are useful in the description of vulnerabilities that are related to E-Government systems and E-Government system security. Figure 7.13 presents a diagram on the vulnerability module within the ontology and its relationship with other key concepts (IT Asset, Threat, Risk).

Vulnerability and *existsOnITAsset some* IT_Asset
Vulnerability and *enablesThreat* some Threat
Vulnerability and *generatesRisk* some Risk
Vulnerability and *increasesVulnerability* some Vulnerability

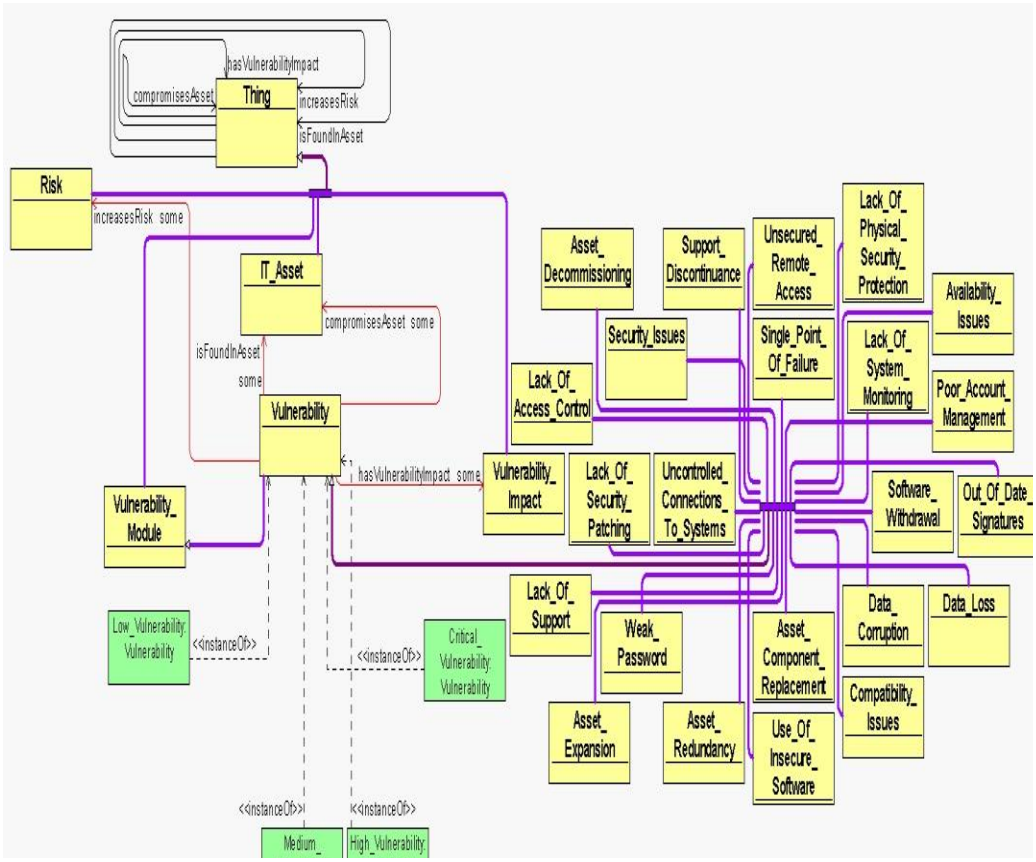


Figure 7. 13: Subset of Vulnerability Modelling in the Ontology with Example

7.5.4.3 Developing the Security Module of the Ontology: Risk Modelling

Figure 7.14 presents a diagram on the risk modelling within the ontology and the relationship the Risk module has with other modules. It also shows the types of risks that are considered in relation to evolution in the ontology. Figure 7.15 presents a subset of the high-level risks that are modelled in the ontology.

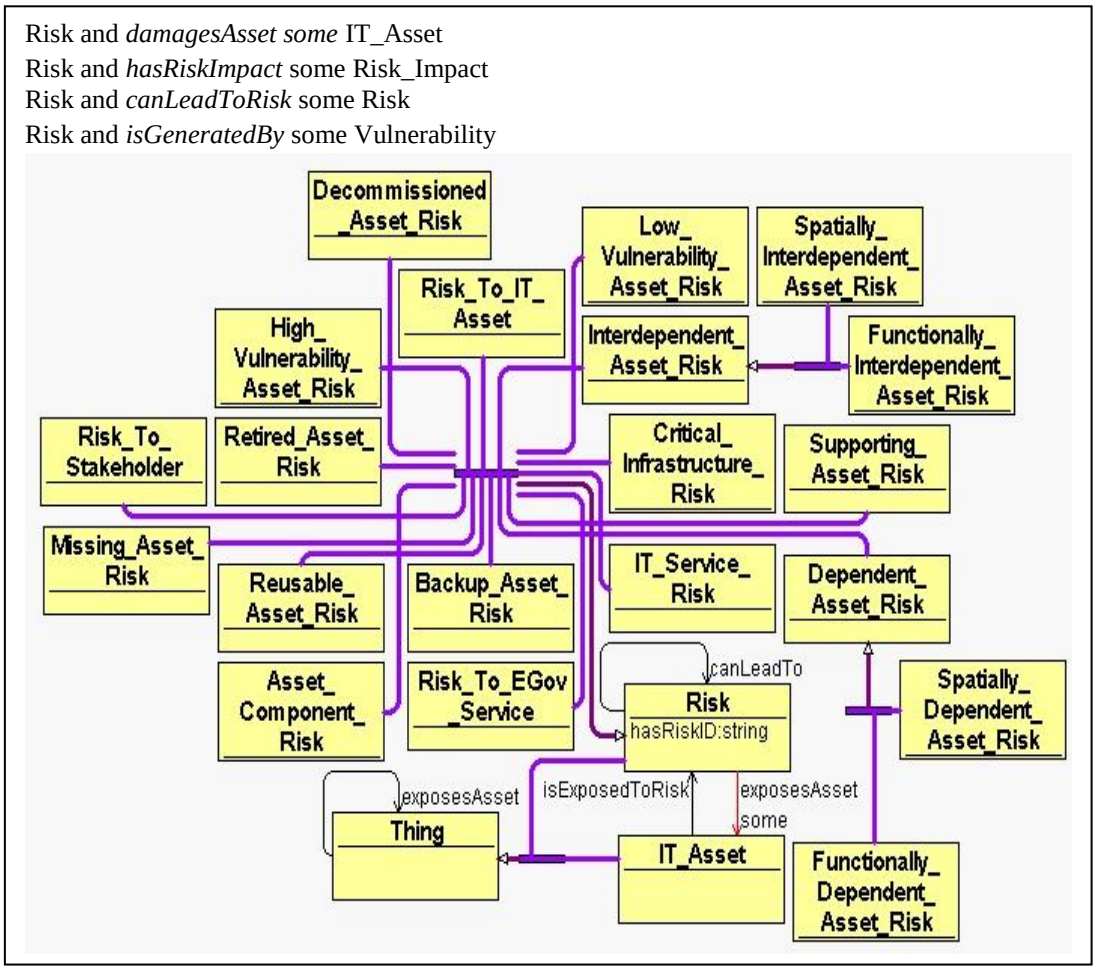


Figure 7. 14: Overview of Subset of Risks Represented in TRAO

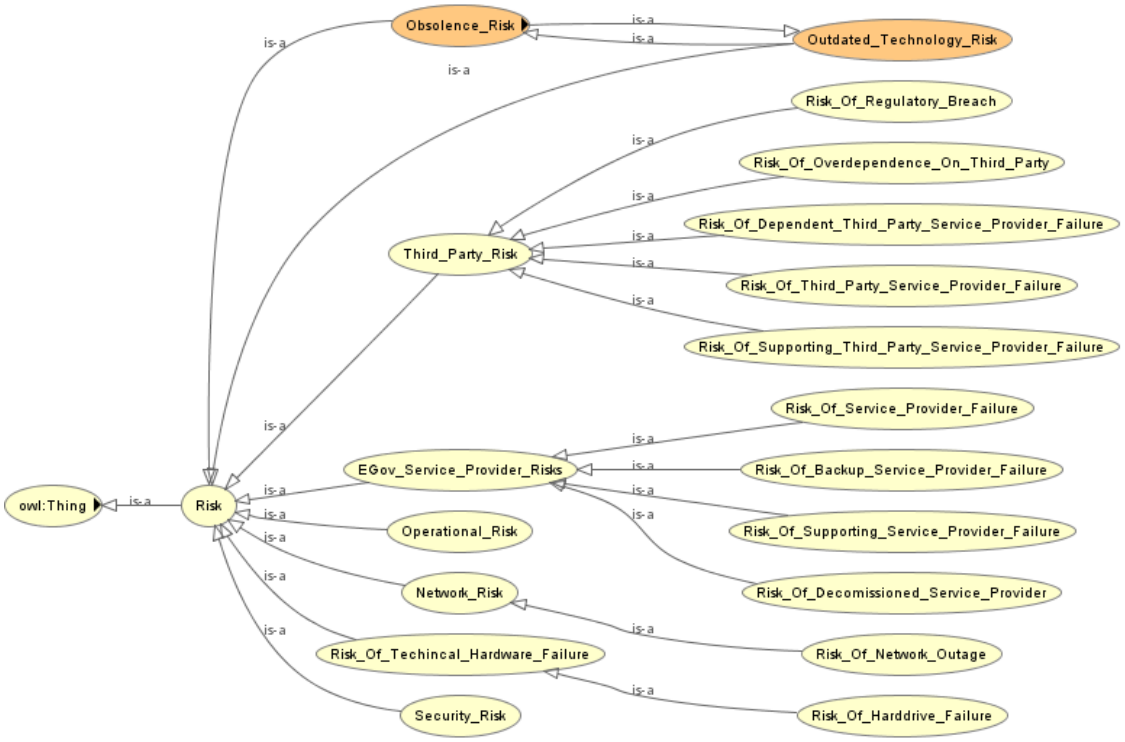


Figure 7. 15: Subset of Examples of Risk Categories in the Ontology using Ontoviz

7.5.5 Risks Associated with Modelling Composite EGov Services

Composite services can be distributed or dynamic services that can create new opportunities to E-Government or further expose E-Government to threats. This thesis posits that the area of coverage for composite services are broader and this is because of their distributed and dynamic nature. Thus, the risks, attacks and threats they are exposed to are more considering that there are several exposures to a risk, threat or attack to take advantage of. While modelling composite services in the ontology, characteristics of composite services had to be taken into consideration. As discussed in 3.4.4, one of the fundamental concepts in SOA is combining smaller services to create complex ones. Thus, this thesis defines a composite EGov Service as the integration of multiple EGov Services. It can also be defined as the integration of multiple EGov Service components. However, composing services together comes with associated evolving threats. The rule of thumb also suggests that a composite service can contain a smaller composite service or an atomic service.

Therefore, logically a composite EGov Service can be defined thus:

$$CS_1 + CS_2 + CS_3 \ldots\ldots\ldots\ldots CS_n$$

7.6 Scenario-based Design of the Ontology

The scenarios in this section are derived from discussions with stakeholders to reflect the usefulness of the ontology. They are developed in the form of interpretive case studies. The background of the development of the ontology is presented using these scenarios. No application is self-sufficient. Thus, there is reliance across applications and systems. The scenarios presented in this section serve as the basis for the development of more complex scenarios which are presented in appendix IV.

In this section, three example scenarios are used to illustrate the applicability of the ontology in different projects.

Scenario 1: The EGov composition scenario - This is used to describe the SP concept and includes the underlying structure of government organisations and their functional units. Furthermore, the provision of EGov Services is dependent on the use of IT Assets. A major focus of the scenario is in being able to perform complex queries in the form of integrated EGov Services based on the composition of government organisations and being able to analyse and evaluate the consequences behind this. These are presented in Sections 7.6.1.

Scenario 2: Asset Composition - Risk scenario - This is used to describe the assets that are used by EGov Services and the special categories of assets (outdated, obsolete, complex assets, dependent and supporting assets). These scenarios are presented in sections 7.6.2, 7.63, 7.6.4, 7.6.5, 7.6.6 and 7.6.7. A main goal of modelling this is to evaluate the risks of using such categories of asset within government and the associated impacts.

Scenario 3: Evolution scenario - This group of scenarios are used to model the risks associated with evolution such as integration of assets or EGov Services. These are presented in sections 7.71 and 7.72; risks associated with the integration of legacy assets with existing assets 7.7.3 and the risks associated with asset reuse.

7.6.1 Driver's License Application – Hypothetical Scenario to Show what Assets a Service Requires to Run

In order to illustrate the TRAO model on a real-world case scenario, a use case for applying and issuing of driving licenses in the UK is described. This is in line with Scenario 2. This use case is used as one of the running examples in this research. Describing a generic use case for issuing of driving licenses, the Driver and Vehicle Licensing Agency (DVLA)

which works with the Department for Transport is assumed to be the SP. A citizen who is the receiver of the service in this case interacts with this system. There are certain relationships the Department for Transport may have with other SPs such as the Driver and Vehicle Standards Agency (DVSA). The Drivers Licence Application which is the system SRs use to apply for a driving license (EGov Service runs on Operating Systems and might even make use of database(s), Web Server or even a high-level application framework. It is equally important that all the code that an application depends on are documented. So, for example, the Driving License application may depend on the following:

1. Web-based client using Microsoft Internet Explorer 6.0 or later and Firefox 1.5 or later
2. Windows 7
3. Microsoft Windows Server 2002 and Solaris 10 servers
4. On the server only, Microsoft SQL Server 2005 (on Windows Server 2003) and Oracle 10g (on Solaris 10)
5. On the server only, Microsoft Message Queue 2.0
6. Microsoft .NET Framework 2.0 and common language runtime 2.0 (server only)

The relationships that exist in this scenario are presented in figure 7.16 and can be retrieved with the following queries in Table 7.8:

Table 7. 8: Queries Relevant to the DVLA Service

Question	**Query**
What assets are required by the Driver's License Application Service?	IT_Asset and isRequiredBy some {DriversLicenceApplicationService}
What departments work with DVLA?	Service_Provider and worksWith some Service_Provider
What Asset components make up the IT_Assets used in DVLA?	Asset_Component and isPartOfAsset some IT_Asset
Who is the recipient of the Driver's License Application Service?	Service_Receiver and receivesEGovService some Driver's License Application Service?

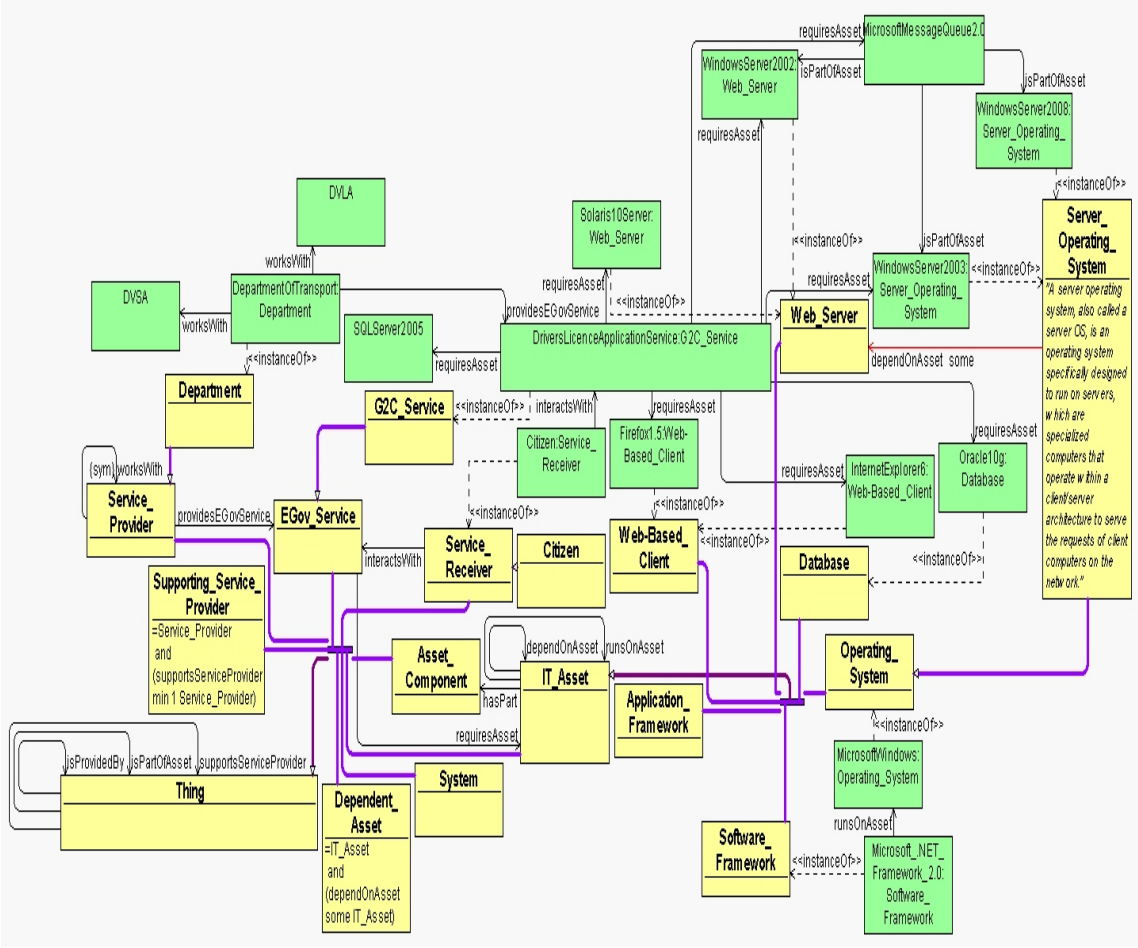


Figure 7. 16: Scenario Modelling of the Driving License Application Service

7.6.2 Hypothetical Scenario- Modelling the Risks of using Outdated/Obsolete Assets

There are different issues that must be considered with the Scenario 2. One of them includes understanding the risks associated with running an EGov Service on an outdated asset. This is in line with scenario 1 and 2. Table 7.9 presents the query that can retrieve these risks

Table 7. 9: Query for Retrieving Risk of using Outdated Assets

Question	Query
What are the risks of running an EGov Service on outdated operating systems and servers?	EGov Service and runsOnAsset some (Outdated_Operating System and Server)

Table 7.10 presents the security considerations for outdated assets in the scenario while Figure 7.17 presents the results of the query. Imagine the case of DVLA's business information being entrusted to a decade-old server and the impacts this will have on the DVLA and its service provisioning. Many companies are still running on Windows Server 2003 (which reached end of service in 2015) or SQL Server 2005 (which reached end of service April 12, 2016).

Table 7. 10: Security Considerations for Outdated Asset

Asset	**Vulnerabilities**	**Threat**	**Risks**	**Risk Impact**
Windows Server 2003 Windows Server 2002	Security Vulnerabilities and Network vulnerabilities. e.g. a. No critical updates and patches on these servers b. No official/technical support c. Incompatibility issues d. Support discontinuance e. 3rd Party Software No Longer Supporting Your Operating System	Security Threat ->* a. Cyber attack Network Failure	Risks of using outdated assets ->* a. Security Risk b. Compliance Risk c. Data breach risk d. Ransomware e. Risk of downtime	a. Financial Impact b. Reputational Impact c. EGov Service Discontinuance d. Decreased SP productivity

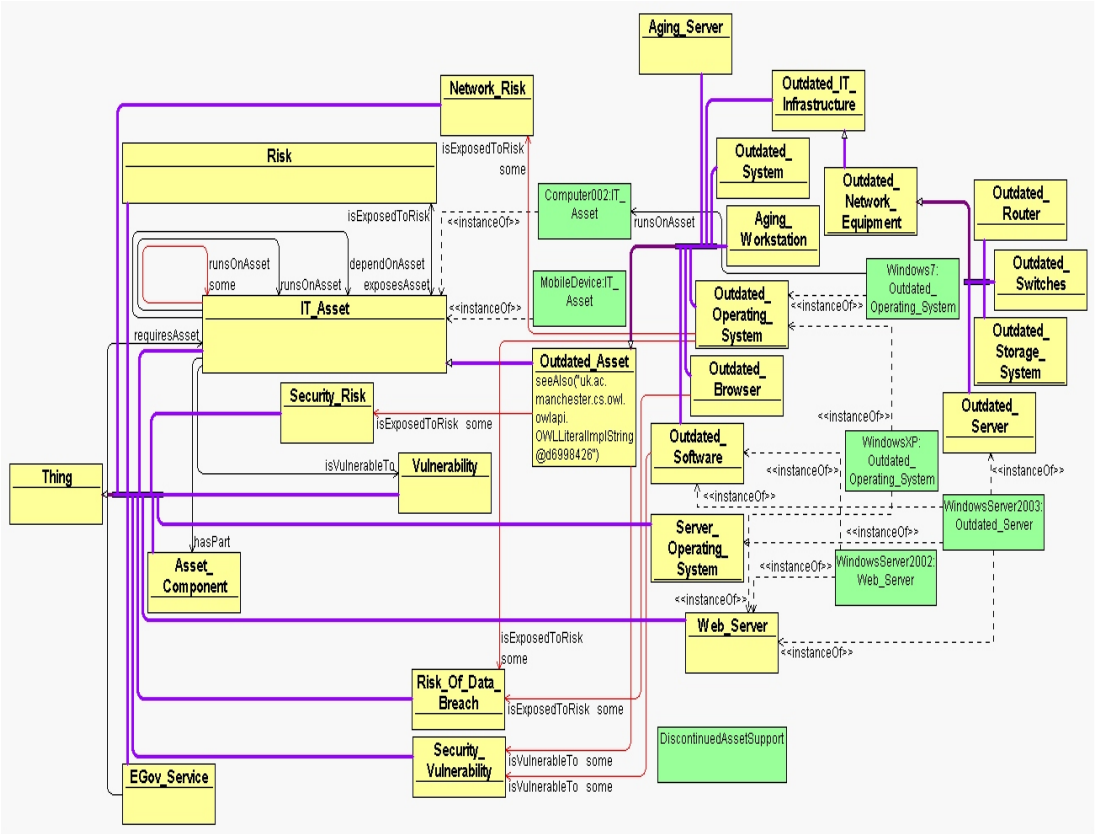


Figure 7. 17: Scenario Modelling of the Security Considerations for an Outdated Asset

7.6.3 Hypothetical Scenario - Modelling the Risks Associated with Moving from an Older Asset to a Newer Asset

Another issue with the DVLA scenario in 7.6.1 is understanding the kind of risks that may occur if an asset migration has to take place from an older asset to a newer asset. Table 7.11 presents query for migrating an older asset to a newer asset. This is in line with scenario 1 and 2.

Table 7. 11: Query to Migrate an Older Asset to a Newer Asset

Question	Query
What vulnerabilities may exist and what are the risks of migrating data or information from an older version of O/S to a newer O/S version while running the DVLA Application Service?	Outdated_Asset and isMigratedTo IT_Asset and isVulnerableTo some Vulnerability and isExposedToRisk some Risk

Table 7.12 presents the vulnerabilities and risks that may occur if consideration is given to migrating from windows 7 to windows 10.

Table 7. 12: Migration Scenario

Scenario	**Query**	**Vulnerabilities**	**Risk**
Migrating from Windows 7 O/S to Windows 10 O/S	{Windows 7} and isMigratedTo only {Winodws10} and is VulnerableTo some Vulnerabilty and isexposedToRisk some Risk	a. Incompatibility with existing hardware b. Incompatibility with existing software c. Insufficient disk space	a. Risk of downtime b. Risk of data loss c. Risk of failure

Further queries can be asked based on the migration scenario such as: *Are there any considerations for the default system-hardening configuration? For example, in the case of Windows Server 2003, one might require only the default hardened version of the operating system to run. Or perhaps one might need to loosen some of the security settings in the system. What happens if neither of this are carried out?*

This is summarised in table 7.13.

Table 7. 13: Security Consideration for Outdated Asset Windows Server 2003

Asset	Vulnerabilities	Risk	Risk Impact
Windows Server 2003	a. Default hardened O/S Unavailable b. Tightly coupled security settings c. Too old d. Unnecessary applications running e. Drives not defragmented f. Unavailable restore points g. Operating system not up to date	Security Risk -> a. Data Leakage	a. Data Loss b. Unrecoverable Active Directory

7.6.4 Hypothetical Scenario to Show the Risks Associated with Complex Assets

A hypothetical scenario coined from the driving license application describes a case where the DVLA has to make use of some complex systems. The complex systems described in

this scenario are ERP systems, CRM Systems and Content Management (CM) Systems, Operations Support Systems (OSS) and Business Support Systems (BSS). These systems evolve and grow in disparate ways with the use of heterogenous technologies and data models. Considering that communication must take place between these systems so that information can be exchanged, the following must be taken into consideration: A Service Provider uses min 1 IT_Asset and an EGov Service requires IT_Asset to run. Tables 7.14, 7.15, 7.16 presents the different questions that can be asked.

Table 7. 14: Query on Assets used by the DVLA

Question	Query	Result
DVLA and usesAsset some IT_Asset	DVLA and usesAsset some ITAsset	DVLA usesAsset some {CRM_System, ERP_System, Content_Management_Systems, Operation_Support_System, Business_Support_System}

Most existing OSS Systems are made up of common components. For the purpose of clarity, only the Assets that make up the Operation Support System will be discussed. The components that make up the OSS System as modelled by the ontology are represented in table 7.15:

Table 7. 15: Modelling Asset Components that Make up as Asset

Question	Query	Result
What components make up each of the assets that are used by the DVLA?	DVLA and hasPart some AssetComponent	(hasPart some Catalog_System) and (hasPart some Inventory_System) and (hasPart some Order_Management_System) and (hasPart some Provisioning_System) and (hasPart some Activation_System) and (hasPart some Message_Queue) and (hasPart some EAI_Middleware) and (hasPart some Subscriber_Directory_Systems) and (hasPart some

		Number_Management_Systems) and (hasPart some Field_Service_Management_System)

It is also important to understand the functions that may be compromised if there are issues with an asset. Table 7.16 presents the functions an asset supports. For the purpose of clarity, only the functions that the OSS System supports are described.

Table 7. 16: Modelling the Support Function of an Asset

Question	Query	Result
What functions does an Asset Support?	OSS_System and (supportsFunctions some Function	OSS_System and (supportsFunctions some Network_Configuration) and (supportsFunctions some Network_Inventory) and (supportsFunctions some Fault_Management) and (supportsFunctions some Service_Activation) and (supportsFunctions some Service_Provisioning

Based on the modelling that an asset can be dependent on one or more assets, Table 7.17 describes the assets that are dependent within the DVLA

Table 7. 17: Queries Relating to Dependent Asset in the DVLA

Question	Query	Result
What are the dependent assets that exist in the DVLA?	DVLA and makesUse of Asset some Dependent_Asset	OSS_System and dependOnAsset some {BSSSystem}.

Thus, this makes the OSS_System a dependent Asset and the {BSSSystem} a Supporting Asset.

Considering that the *hasPart* relationship is a transitive relationship in the ontology. The following question can be asked: ***What other systems are linked to the OSS_System***

The Provisioning System which is a part of the OSS_System has an important Asset component known as the Provisioning Logic. Thus, running a query to know the asset components of the Provisioning Logic returns a result of the OSS_System. This description sets the precedence on debates of modelling cascading impacts such as failure on Assets and Asset components.

Figure 7.18 provides a diagram showing the high-level modelling of this scenario and Figure 7.19 provides a query in relation to the transitivity property of this asset and its component parts

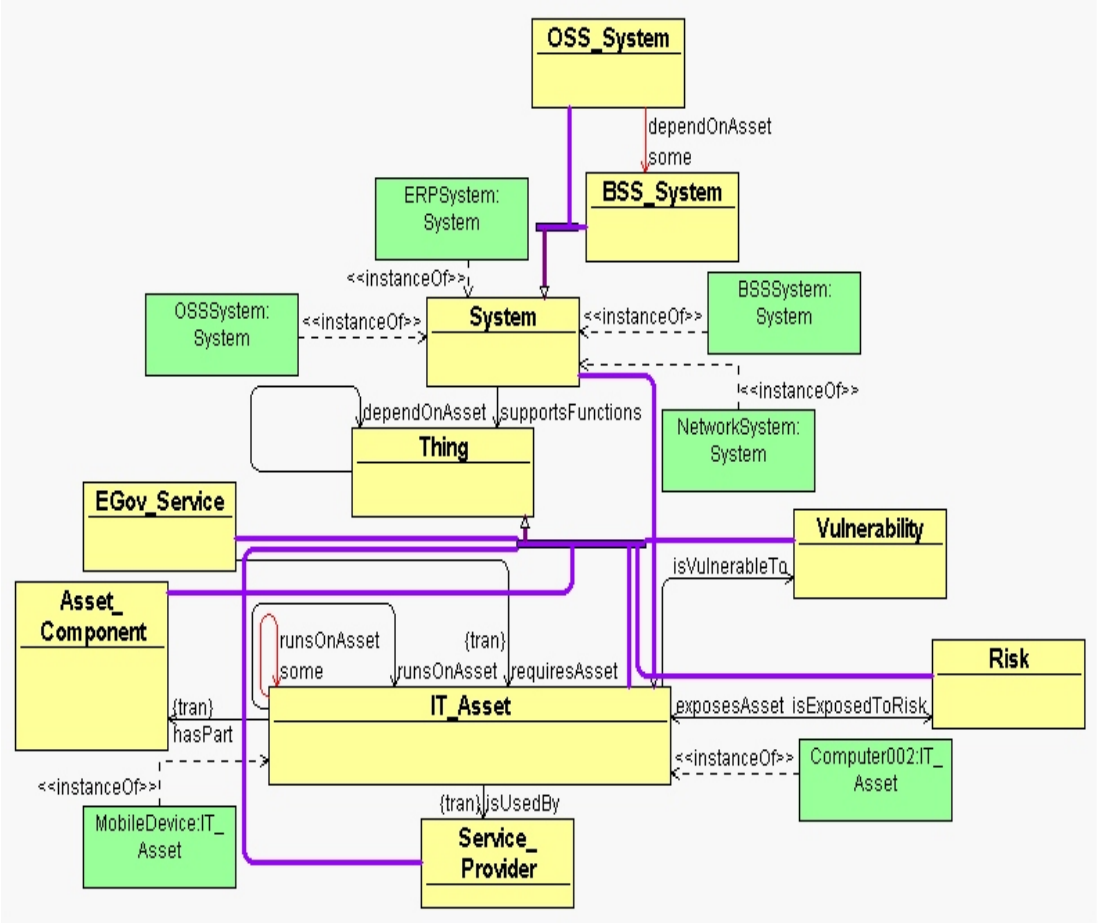


Figure 7. 18: Scenario Modelling Showing Risks Associated with a Complex Asset

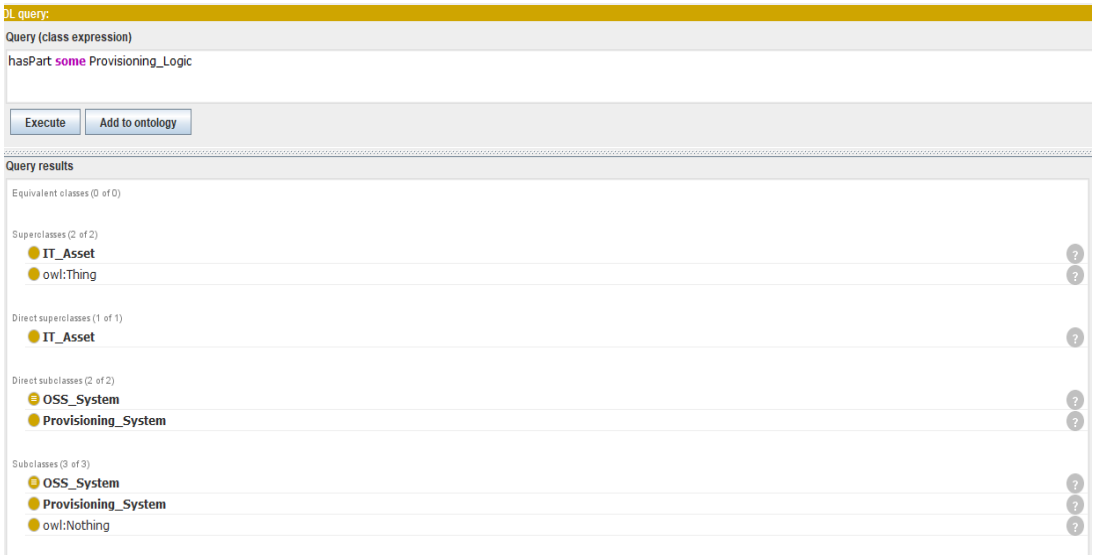


Figure 7.19: Scenario Modelling of the hasPart Transitive Relationship

7.6.5 Hypothetical Modelling of Assets that Act as Dependent and Supporting Systems

The ontology models the OSS_System which is dependent on the BSS_System. However, this system also acts as a supporting asset given that it supports Network Systems in the DVLA. Figure 7.20 provides a query showing that a Supporting Asset can also be a Dependent Asset

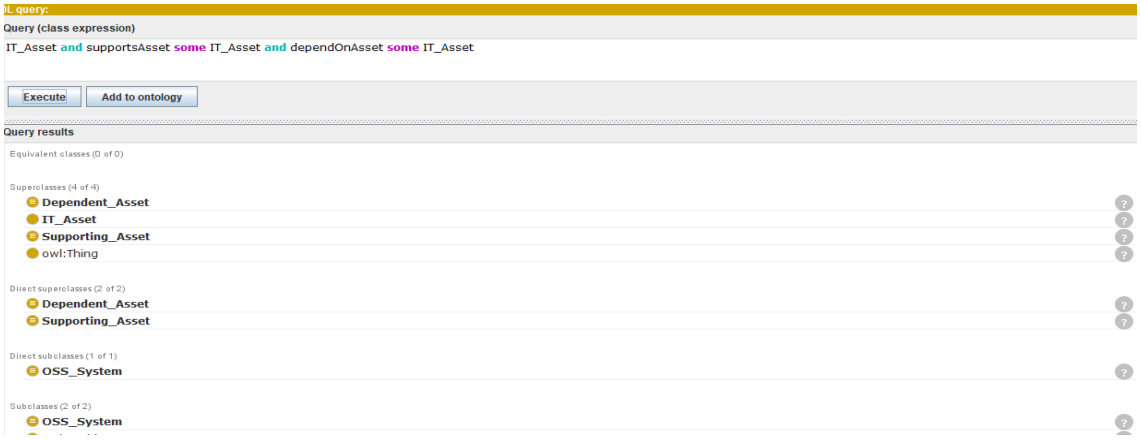


Figure 7. 20: Query Showing that a Supporting Asset can also be a Dependent Asset

However, the risks associated with having a Supporting Asset as a Dependent Asset have to be considered. Table 7.18 presents the query on this.

Table 7. 18: Query to Support Dependent and Supporting Assets

Question	Query
what are the risks that an asset that is both a supporting and dependent asset exposed to?	Risk and *exposesAsset* some IT_Asset and (Supporting_Asset and Dependent_Asset)

7.6.6 Hypothetical Network Scenario Describing Reliance on a Network and the Cascading Effects of this Reliance

A hypothetical Department (D2) in government has a network {Network004} which is used for different purposes where different departments (D1, D4, D6) rely on this network to deliver various EGov Services. The components of this simple network include the following assets: subnet LAN with about 50 hosts (with PCs), 1 database server, 1 file server, 1 print server, one Active Directory (Domain Controller – DC) server a layer three switch, a router and a firewall (for an Internet connection and VPN), as well as 2 administrators running the show. Based on this network scenario, the following assets exist when broken down into components:

- 50 PCs with end users connected to them and the applications they run
- Systems – 4 servers (file/print/database and directory)
- Network and security Infrastructure – switch, router and firewall
- 2 administrators
- The data contained on the systems deemed valuable

Table 7.19 presents a query to show what asset is reused by some SPs.

Table 7. 19: Asset Reuse Query

Question	Query	Result
What asset is used by different departments	IT_Asset and isReusedBy some Service_Provider	Network004

Table 7.20 presents a query on the SPs that use Network004

Table 7. 20: SP Reuse Query

Question	Query	Result
What SPs make use of Network004	Service_Provider and reusesAsset only {Network004}	{D1}, {D4}, {D6}

Table 7.21 presents a query to show the components of Network004

Table 7. 21: Query to show Components of an Asset

Question	Query	Result
What are the components of Network004	{Network004} and isMadeUpOfComponent some AssetComponent	{50PCs} {File_Server} {Print_Server} {Directory_Server} {Network Infrastructure} {Data}

Table 7.22 presents the security considerations for some of the assets.

Table 7. 22: Security Consideration for Assets

Question	Query
What are the vulnerabilities, threats risks, and risk impacts associated with the Network Print Server of Network004?	{Network_Print_Server} and *isVulnerableTo* some Vulnerability and *isThreatenedByThreat* some Threat and *isExposedToRisk* some Risk and *hasRiskImpact* some Risk_Impact

The results of this query are presented in Table 7.23

Table 7. 23: Results of Security Consideration Query

Assets	Vulnerabilities	Threats	Risk	Impacts
Network Print Server	Server connection failure	Failure of print server	Security Risk	Additional network traffic

Furthermore, considering that {D1}, {D2} and {D6} have to reuse {Network004} that already has a vulnerability in it (V1, V3) and is threatened by threats (T1, T2). It may be forced to inherit the vulnerabilities of the software asset which can lead to various risks.

7.6.7 Scenario Modelling of IT Asset Failure

What happens to any failed asset considering that there are dependencies that exist among them?

There are multiple ways in which an asset can fail. This thesis models the following failure modes in the ontology:

i. Dependency Failures: This is modelled in the form of complex assets (systems) where a system is made up of a number of interacting components. Thus, the failure of an asset component can cause the destruction of other asset components which may eventually destroy the complex asset. In modelling this type of failure, examples are modelled using end of life /outdated/aging asset components and dependent components
ii. Internal Dependency Failures: This is modelled in the form that certain components are critical to the successful delivery of an EGov Service.
iii. Cascading Failures: This is modelled in the form that a failure of an asset or asset component can trigger or cause the subsequent failure of another asset or component.

Table 7.23 presents a modelling of the dependencies that exist between assets in the scenario.

Table 7. 24: Dependencies that Exist between Assets

S/No	Asset	Dependencies

1	Microsoft Messaging Queue 2.0	isPart of Asset {Windows 2003} isPart of Asset {Windows 2002} isPart of Asset {Windows 2008}

7.7 Scenario Modelling of Risks

According to the Department of Environmental Affairs in South Africa, risks can be identified using a variety of approaches such as: checklists, judgements based on records and experience, flow charts, systems analysis, system engineering and scenario analysis. The scenario analysis approach has been adopted for identifying risks and modelling what has been identified using an ontology (DEA 2013).

7.7.1 Risks Associated with Combining Individual/Atomic EGov Services

Individual/ atomic EGov Services exist in government such as in the NHS. To enhance productivity, there are cases where these atomic services have been combined. However, combining these atomic services comes with associated risks based on the assets that they make use of. Logically this is represented thus:

$$S_1 + S_2 + S_3 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, Sn \rightarrow CS_1$$

This thesis also posits that to combine atomic EGov Services, the assets and components that make them up may need to be combined. Similarly, these assets and components may have associated risks. Some of these components may also be composite while some may be atomic. Atomic components or services should be indivisible. Figure 7.21 presents a diagram on the integration of atomic EGov Services (S_1, S_2, S_3…. Sn) to achieve a composite service CS_1.

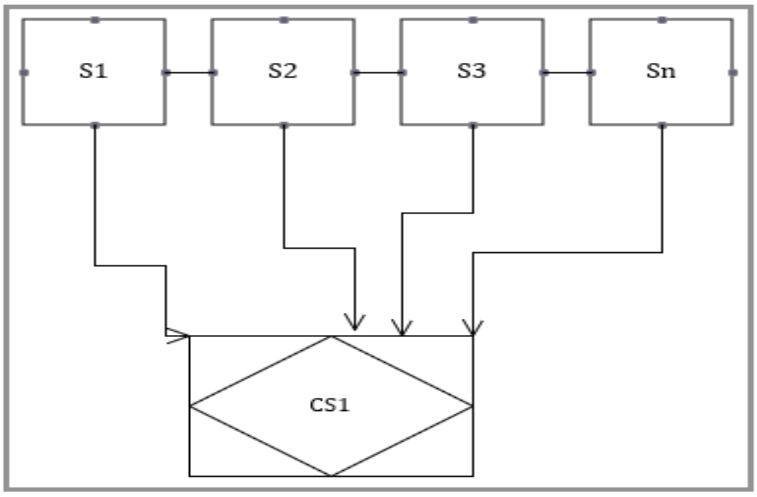


Figure 7. 21: Integration of Atomic E-Government Services to create Merged EGov_Service

As a running example, the NHS has attempted merging the Care Service and the Health Service. However, this ontology takes into consideration the following: (i) the platform an EGov Service is built on; (ii) the risks a platform is exposed to; (iii) the risks associated with merging the two EGov Services; (iv) the accumulated risks associated with merging these EGov Services. This is presented in Table 7.25.

Table 7. 25: Query showing the Platform an EGov Service

Question	**Condition**	**Query**	**Result**
What are the platforms that the Care Service and Health Service run on?	An EGov Service is built on a platform.	{Health_Service} and {Care_Service} and isBuiltOnPlatform some Platform	{Health_Service} and *isBuiltOnPlatform* {P3} {Care_Service} and *isBuiltOnPlatform* {P1}
What risks are the Health Service and Care Service platforms exposed to?	A Platform is exposed to individual risks	{P3} and {P1} and *isExposedToRisk* some Risk	{P3} and *isExposedToRisk* some {P3_Risk} {P1} *and isExposedToRisk* some {P1_Risk}

Question	Condition	Query	Result
What are the risks of merging two EGov Services	Merged_EGov_Service = EGov_Service and *isMergedWith* min 1 EGov_Service Merged_EGov_Service and *isExposedToRisk* some Merged_EGov_Service_Risk	{Health_Service} and *isMergedWithEGovService* some {Care Service} and *isExposedToRisk* some Risk	{Health_Service} and *isMergedWithEGovService* some {Care Service} and isExposedToRisk some Merged_EGov_Service_Risk
What are the combined risks that merging the Health Service and the Care Service are exposed to?			Merged_EGov_service {HealthService; Care_Service} and *isExposedToRisk* some ({P1_Risk}; {P3_Risk}, Merged_EGov_Service_Risk)

7.7.2 Hypothetical Scenario Modelling of the Dependencies/Interdependencies that Exist Among Assets

There are different relationships that are used to model relationships within the ontology such as: functional dependent/interdependent relationships, spatially interdependent relationships, mutual interdependent relationships. The different types of relationships described in table 3.3 are used to develop scenarios based on these relationships.

1. Functional Dependency: The ontology models this dependency in the form of an entity relying on another entity to operate in a certain way. Thus, an IT_Asset may be functionally dependent on another IT_Asset.

Functional dependency ITA_1 -> ITA_2 when ITA_2 **is functionally dependent on** ITA_1 (Therefore, ITA_1 is the **determinant entity** and ITA_2 is the **dependent entity**). This is shown in the case where an Asset ($ITA_{2)}$ may depend on another Asset ($ITA_{1)}$ but ($ITA_{1)}$

does not depend on ($ITA_{2)}$. This relationship also applies to Service_Providers. A typical case of this kind of relationship is also seen with the DVLA being functionally dependent on the Department of Transport. Thus, making the DVLA a Functionally_Dependent_Service_Provider.

7.7.3 Hypothetical Scenario to Show the Risks Associated with Merging Legacy Assets

Attempts have been made to merge the Legacy systems of the Drivers Licence Application System which are the ERP Systems, CRP Systems and CM Systems. The following must be considered.

i. Sequel to a successful migration as discussed in 7.6.3, what happens if at the end of the migration, DVLA realizes that the CRM or ERP systems are not compatible (Vulnerability) with the new OS? This leads to a case of legacy system risks.
Query: IT_Asset and *isMergedWith* some Legacy_Asset
Figure 7.22 presents a diagram that returns a result for this query

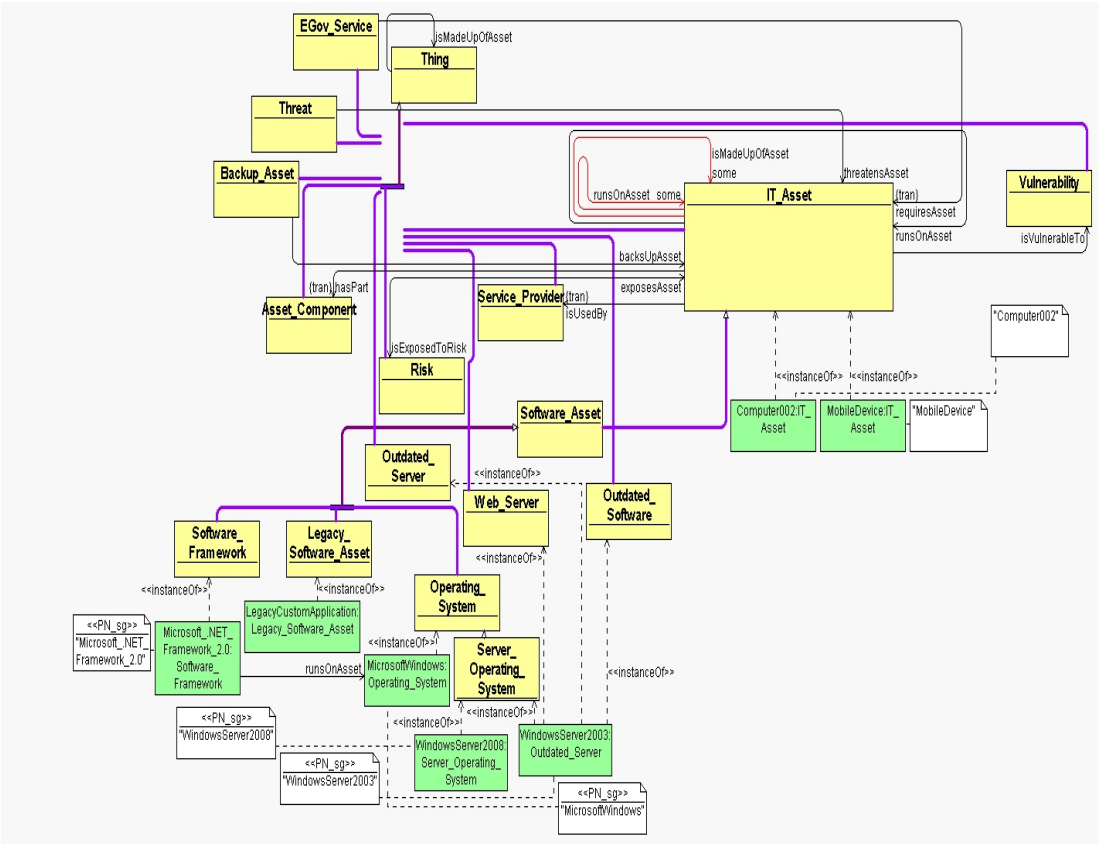


Figure 7. 22: Modelling of Ontology showing Risks Associated with Merging Legacy Assets

7.8 Rule Formulation for TRAO

In addition to the development of the ontology, rules were developed to extend the inference functionality within TRAO. This was achieved using the Semantic Web Rule Language (SWRL). A subset of inference rules used within the ontology are presented in table 7.26. These rules can be applied on every instance in TRAO.

Table 7. 26: Subset of Rule Formulation

AttackPatternClassification: IT_Asset (? x) ^ existsOnAsset(?y, ?x) ^ exploits(?z, ?y) --> related_to(?x, ?z)
Dependent_Asset: IT_Asset(?i) ^ dependsOnAsset(?i, ?d) ->:Dependent_Asset(?i)
Fourth_Party_Service_Provider: Third_Party_Service_Provider(?t) ^ reliesOnThirdPartyServiceProvider(?t, ?s) ->: Fourth_Party_Service-Provider
Fourth_Party_Service_Provider_Risk: Third_Party_Service_Provider(?t) ^ reliesOnThirdPartyServiceProvider(?t, ?s) -> Fourth_Party_Service_Provider_Risk(?t)
Service_Receiver: Stakeholder(?x) ^ receivesEGovService(?x, ?y) -> Service_Receiver(?x)
Threatened_Asset: IT_Asset(?i) ^ isThreatenedBy(?i, ?x) -> Threatened_Asset(?i)
Vulnerable_Asset: Vulnerability(?v) ^isFoundInAsset(?v, ?a) -> Vulnerable_Asset(?a)

Impacted_Asset: Vulnerability(?v) ^ isFoundInAsset(?v, ?a) -> Vulnerable_Asset(?a)

7.9 Query Formulation in TRAO

The development of queries that are structured is a meaningful way to access data since it allows for complex query formulation. Queries were developed to aid the retrieval of specific data from the large amount of data contained in TRAO. Two types of queries are used within the ontology and they are described in sections 7.91 and 7.9.2.

7.9.1 TRAO DL Queries

DL Queries are OWL class expressions and are designed to work with OWL ontologies. Thus, they have a native understanding of the semantics of OWL and can handle the many constructs in an OWL ontology. It is however only made available in Protégé and is known to have a compact notation. The query results in DL can be in the form of Superclasses, Subclasses or individuals of the expression of a class. Its inability to perform comparisons between different variables or use variables makes this language restrictive. Table 7.27 presents a subset of generic Description Logic (DL Query) queries that can be easily run natively on the ontology. More Queries are presented in Appendix IV.

Table 7. 27: Generic TRAO DL Queries

Question	**DL Query**
1. Who provides a service?	Service_Provider and providesEGovService some EGov_Service
2. What Stakeholders or SPs make up the Cabinet_Office?	{Cabinet_Office} and *isMadeUpOfServiceProvider* some Service_Provider

Question	**DL Query**
3. What Stakeholders or SPs is the Government Digital Service part of?	Service_Provider and *hasPart* some {Government_Digital_Service}
4.What SP is responsible for providing Digital_Government_Service?	Service_Provider and providesEGovService some {Government_Digital_Service}
5. Who is responsible for the management of an IT_Asset?	Stakeholder and *managesAsset* some IT_Asset
6. What assets does an EGov_Service require to run on?	EGov_Service and *requiresAssetToRun* some IT_Asset
7. What EGov_Service require particular assets?	IT_Asset and *isRequiredToRun* some EGov_Service
8. How do we show the interconnection between EGov_Services, SPs and IT Assets?	Service_Provider and *providesEGovService* some EGov_Service and *requiresAssetToRun* some IT_Asset
9. Does an EGov Service require more than one asset to be in place?	EGov_Service and *requiresAssetToRun* min 1 IT_Asset
10. What are the risks associated with an EGov Service relying on Third-Party SPs?	EGov_Service and *requiresAssetToRun* some IT_Asset and *reliesOn* some Third_Party_Service_Provider and *isExposedToRisk* some Third_Party_Risk
11. How do you know what it_assets are being used by Third-Party SPs?	IT_Asset and *relyOn* some Third_Party_Service_Provider

Question	**DL Query**
12. How does one know what Government Asset uses a Third-Party SP and what Third-Party assets are in use?	{UK_Verify} and *relyOn* some Third_Party_Service_Provider and *makesUseOf* some Third_Party_Asset
13. what are the risks associated with a system (asset) like the UK Verify relying on Third-Party systems?	IT_Asset and *relyOn* some Third_Party_Service_Provider and is*ExposedToRisk* some Third_Party_Service_Provider_Risk
14. How can it be established which department owns a particular asset for a service to be delivered?	Stakeholder and *ownsAsset* some IT_Asset Stakeholder and *ownsAsset* some{Fostering_Case_File_2015/2016} Stakeholder and *ownsAsset* some{PIE1}
15. What are the risks of a third_party SP relying on another third_party SP	Third_Party_Service_Provider and *dependsOn* Third_Party_Service_Provider and *isExposedToRisk* some Third_Party_Risks
16. What are the risks associated with dependencies of single/complex systems, components or infrastructures?	Complex_Asset and *dependsOnAsset* and *isExposedToRisk* some Complex_Dependent_Asset_Risk
17. What are the risks associated with interdependencies between complex systems?	Complex_System and isInterdpendentOnAsset some Complex_System and isExposedToRisk some Complex_Interdependent_System_Risk
18. What are the risks associated with complex assets?	Complex_Asset and isExposedToRisk some Complex_Asset_Risk

7.9.2 SPARQL Query Formulation

SPARQL queries are referred to as the query language of the Resource Description Framework (RDF) and are used for some querying of the ontology. They allow for queries to be done in triples. Considering that OWL ontologies have the possibility of being serialised, they can be serialised as RDF. The use of SPARQL queries in the ontology is because of the wide availability of SPARQL engines which have significant adoption.

1. Query to know what EGov Services run on a platform e.g. what EGov Service runs on P3?

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
SELECT DISTINCT *
WHERE
{?x ?y <http://www.semanticweb.org/owner/ontologies/2018/6/untitled-ontology-46#P3> }
```

2. Query to know what Assets are composed of other assets e.g. what assets make up AC1?

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
SELECT DISTINCT *
WHERE
 {?x ?y <http://www.semanticweb.org/owner/ontologies/2018/6/untitled-ontology-46#AC1> }
```

3. Query to show what services are merged together e.g. what services are merged with EGS1

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
SELECT DISTINCT *
WHERE
 {?x ?y <http://www.semanticweb.org/owner/ontologies/2018/6/untitled-ontology-46#EGS1> }
```

4. Query to show what distinct assets a particular asset may depend on

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
SELECT DISTINCT *
WHERE
 {?x ?y <http://www.semanticweb.org/owner/ontologies/2018/6/untitled-ontology-
 69#CRMSystem> }
```

5. Query to show what SP uses a particular system/asset

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
SELECT DISTINCT *
WHERE
{?x ?y <http://www.semanticweb.org/owner/ontologies/2018/6/untitled-ontology-
69#Computer002> }
```

6. Query to show assets that make up the department of health network

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
SELECT ?Dept ?Asset
{<http://www.semanticweb.org/owner/ontologies/2017/11/untitled-ontology-
23#Department_Of_Health_Network> ?Dept?Asset}
```

7.10 Summary

This chapter has introduced the development of an integrated ontology that spans across the E-Government, Security and IT Asset domains. This is done so that data querying at a conceptual level can be supported across the different ontology modules. Furthermore, scenarios have been presented to show the applicability of the ontology and its relevance to the growing research field. More examples of the modelling of the ontology are presented in Appendix VI. Furthermore, this chapter has further answered RQ1, RQ2, RQ3, RQ5 and RQ6.

Chapter 8: Design and Development of TRAO Web-based Tool

There is a need to make accessible to end-users the contents of the Semantic Web and one way to achieve that is to make use of Natural Language Interfaces (NLI). NLIs offer end-users the option of querying ontology-based knowledge bases considering that they can achieve high retrieval performance as well as domain independence (Kaufmann & Bernstein 2007). The need to access data that is structured which exists in the form of ontologies requires the ability to learn formal query languages such as SeRQL and SPARQL (Damljanovic et al. 2008). However, this poses difficulties which are significant for non-expert users and thus requires a process that makes querying of ontologies more straightforward with the use of NLIs. Thus, Chapters 6 and 7 have provided a basis for the development of the TRAO web-based tool. In this chapter, the development of the TRAO prototype tool demonstrates the feasibility of the design if adopted, the functionalities of the tool and how it can be used as a platform for supporting the developed ontology described in Chapter 7. The tool focusses on retrieving queries which are run against the ontology.

8.1 Introduction to TRAO Web-based Tool

The need to organise the tremendous amount of data in E-Government has necessitated the use of vocabularies that are controlled and the use of ontologies that provide computable and consistent languages in the representation of information. The maintenance of ontologies that are large and complex is a non-trivial task and therefore there is the need to have supporting tools and services in place (Sirin *et al.*, 2007).

Studies have shown that the use of NLIs has the ability to hide the formality of query languages and ontologies by offering ways of querying in familiar and intuitive ways (Kaufmann & Bernstein 2007). The development of a query tool is part of the user interface. This guides the user in composing queries. The user interface is responsible for all the interaction a user has with the tool. It allows users to type text and annotations. It shows terms from the ontology and enables users to search for appropriate terms.

Considering that the maintenance of ontologies is a tedious and time-consuming process which poses the risk of the domain expert losing orientation in ontologies that are large, there is need for support with the use of tools which would help in making suggestions that are

reasonable to the ontology developer or automation of tasks that are based on principles that have been outlined ahead of time.

8.2 Functional Overview of the Prototype Tool

The TRAO web-based tool has two major functionalities. The first functionality is the part of the tool that allows a user to run queries while the second functionality allows a user to perform searches over the associated ontology (TRAO).

Figure 8.1 shows an overview of the functionalities of the TRAO web-based tool.

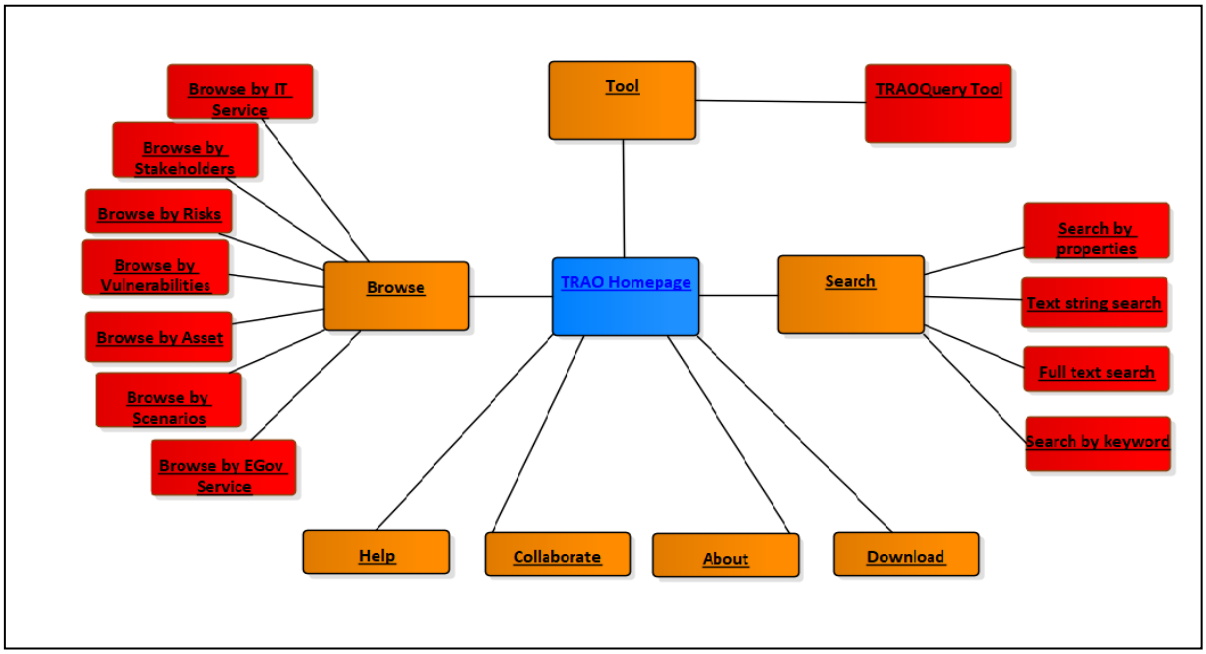


Figure 8. 1: Overview of the Functionalities of the TRAO Web-based Tool

8.2.1 Design Goals

The design goals of the web-based tool are presented in this section and include the following:

1. To efficiently develop a web-based tool that supports querying of TRAO.
2. Provide a NLI that will be easy for users to run queries given they may not be trained in the use of query languages.
3. Present a visual representation of the queries asked in Natural Language and the corresponding results based on those queries

8.2.2 Functional Overview of the Query Aspect of the Tool

This section discusses the functionalities of the query part of the tool. The main functionalities of the tool include discovering whether certain assets can be combined, reused, depended on etc. and the risks associated with these activities. This tool also provides a basic framework and supports the construction of queries that make use of this framework. It enables powerful querying which can be carried out quickly and easily. The diagram in Figure 8.2 provides the core operation of the TRAO query web-based tool.

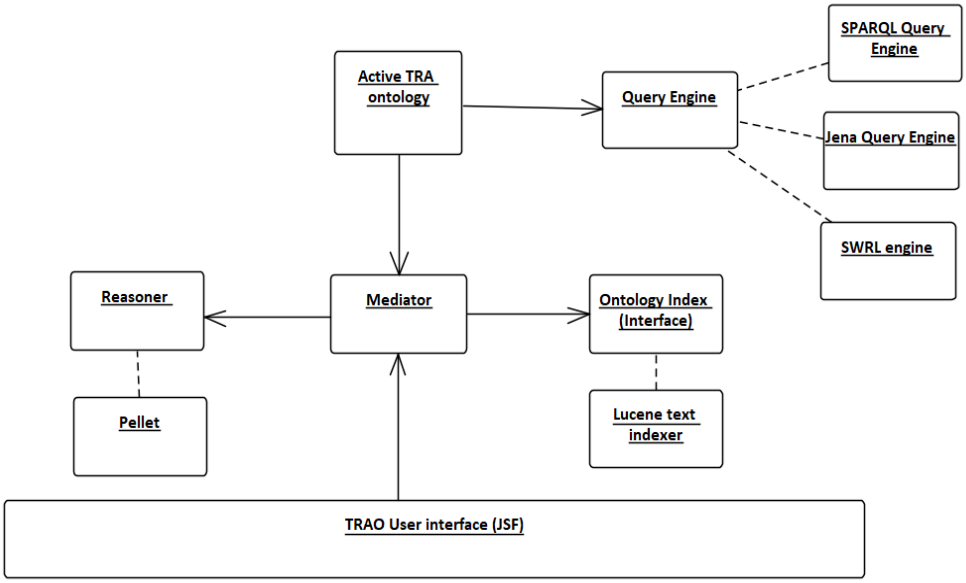


Figure 8. 2: Core Operation of the TRAO Query Tool

TRAO query tool was developed using the Java programming language and it interoperates with other Semantic web technologies such as the OWL API, Protégé, Pellet as well as Jena. The components of the TRAO architecture include the following: a web-based user interface, a semantic web application mediator, an ontology repository, SPARQL, SPARQL query engine. This section describes the components of the TRAO query architecture and the technologies used in its development.

The following section describes the components of the TRAO architecture and the tools that were used in their development.

1. **Development of Client-side interface**: The development of the web-based user interface leverages on the technology of Java Server Faces (JSF). JSF is the standard java

component-based user interface framework used for building web applications[86] and server-side user interface components. It follows the Model View Controller (MVC) design pattern. An object diagram of the MVC showing its features is presented in Figure 8.3.

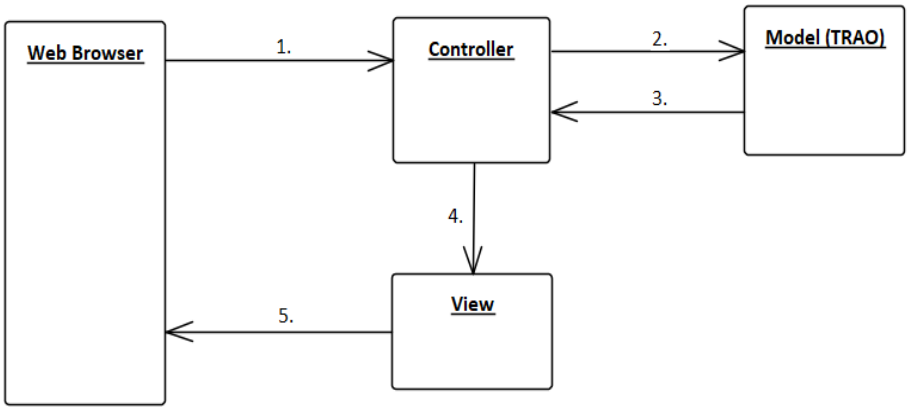


Figure 8. 3: Architecture of the MVC

A description of Figure 8.2 shows that the MVC picks a key functionality of the application and breaks it into smaller components. The Web browser allows a user to make a web request e.g. submit form data, run query etc. This request goes to the controller which controls traffic or routes the request. Thus, the controller chooses which part of the code to execute for a given request. It also accesses the model which provides access to the backend data (ontology). The model handles retrieving and updating data from the backend service. It is responsible for holding all core and logic data. The controller is also responsible for passing the data to the view once this is retrieved from the model which renders a view or HTML response. The view is a page for rendering the results of the SPARQL queries. It displays the content of the application. This includes the query and query result pages.

The choice of JSF for the development of the TRAO web-based tool is based on the following: It provides rich user interfaces over standalone fat clients (Mahmoud, 2004); JSF is extendable because it incorporates Third-Party components which were added to the application; and its ability to manage application states for web requests. A JSF application is composed of components and managed beans which is a regular java class used for holding

[86] JSF technology is a framework for developing, building server-side User Interface Components and using them in a web application. JSF technology is based on the Model View Controller (MVC) architecture for separating logic from presentation.

form data as well as interacting with the backend. An object diagram showing how JSF works in the context of this research is presented in Figure 8.4.

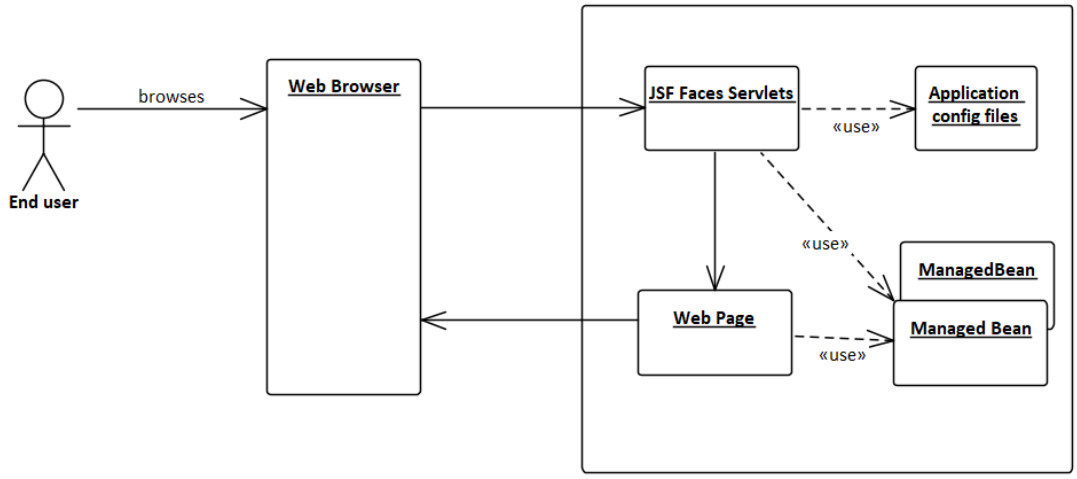


Figure 8. 4: Components and Operations of JSF

A description of Figure 8.4 shows that a user uses the web browser to submit a query to the application server which goes to the JSF faces servlet which is part of the JSF library. The faces servlet handles routing requests to the appropriate pages and determines which page to route to and routes it to the appropriate web page. It also reads information from the config files and makes use of managed beans. The managed beans hold form data and talks to the processes taking place at the backend (TRAO). The web page uses the managed beans to display or retrieve information from the ontology. The web page is rendered and sent back to the web browser based on queries that are input by an end user.

2. **Development of the Servlet engine:** The use of a runtime environment for the development and testing of the JSF application was used. The servlet engine used for this development is Apache Tomcat 8.5.32 available at http://localhost:8080/. This is used to serve the pages from TRAOSearch.

3. **Development Environment (Java IDE)**: The Eclipse Java EE development environment was used for the development.

4. **Semantic Web mediator:** The use of a semantic web mediator was employed based on the need to enable interaction between heterogenous systems and to map data to the ontology. The TRAO mediator is responsible for managing the ontologies used by the TRAO

web-based tool and enables interactions among components and controls the behaviour of the system. The TRAO is loaded using the mediator. It is the loaded ontology that allows reasoning and querying to take place. Thus, it enables communication to take place between the reasoner, the ontology index and the ontology.

5. **Ontology Indexer:** The use of the Lucene ontology indexer is employed to search and retrieve the semantic content of the components of the TRAO. This is done based on the ontological annotations used within the ontology. The ontology indexer is used to enable the fast and easy choice of classes, properties and instances that are used within the ontology. Lucene is a full text search library written in java.

6. **Query engine:** The SPARQL query engine was used to standardise querying of data from RDF sources. It provides the ability to query a triple store repository. In addition to the SPARQL Query engine, the Jena query engine was also used. The use of Jena was employed because of its ability to allow a range of inference engines and reasoners to be plugged into it. The Semantic Web Rule (SWRL) engine was also used to define rules in the ontology.

8.3 Tool Features

The design of the web-based tool requires different questions to be asked so that the different aims and needs of users can be identified. Designing the web-based tool involved answering the following questions:

i. What needs should the tool be able to meet?
ii. What are the functionalities each user needs from the web tool?
iii. What technologies are required to make the tool usable and interactive?

Figure 8.5 presents the landing page of the TRAO web-based tool

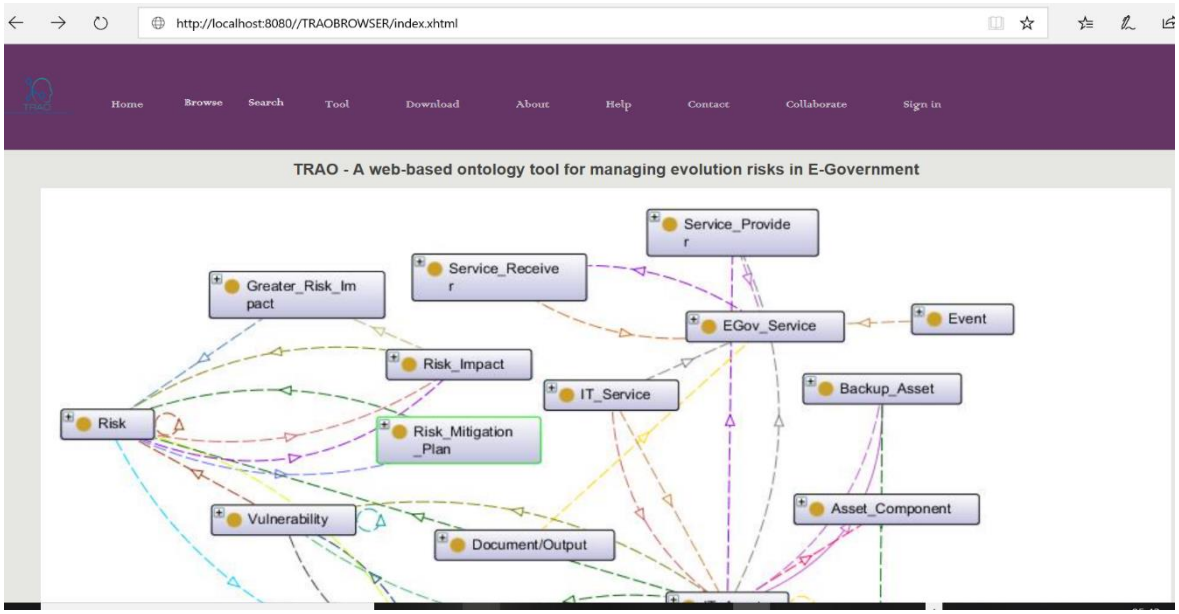


Figure 8. 5: Landing Page of the TRAO Web-based Tool

8.3.1 Ontology Browser

The web-based ontology browser has different features that enable the generation of relevant information from the ontology. The features of the ontology browser are discussed in this section. The ontology browser generates hyperlinked elements from the OWL ontology using the tools menu. This exports the ontology to an OWLDoc and enables an end user browse through classes, subclasses, instances, object properties, data properties etc. All entities can be retrieved using the ontology browser. Thus, the ontology browser allows a user browse through the ontology based on different modules. The TRAO ontology browser allows one to retrieve all Stakeholders, IT Assets, IT Services, EGov Services, Risks, Threats and Vulnerabilities that are annotated to a particular term. The entity to be searched for is found using a drop-down menu. Selecting an entity from the drop-down menu allows for the respective hierarchy of search terms to be automatically loaded in the window. Figure 8.6 provides an overview of the browse functionality of the TRAO web-based tool which shows how a user can browse the ontology based on different modes.

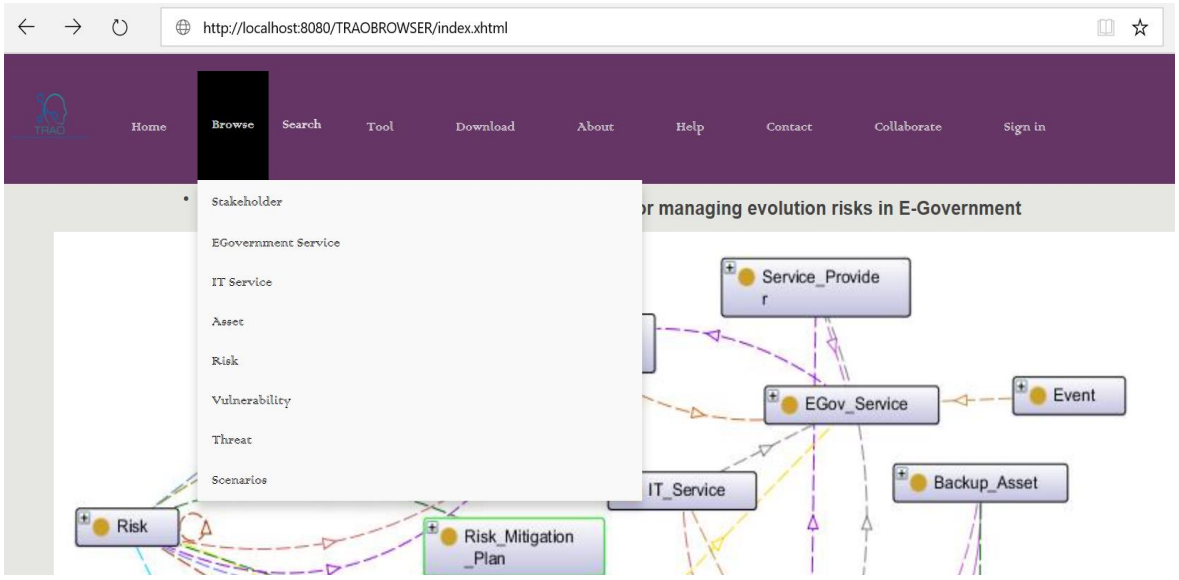


Figure 8. 6: Browse Functionality of TRAO Web-based Tool

The ontology is developed in modules. However, each of these modules is implemented as a mode in the web-based tool. For example, the Threat module in the ontology is referred to as the Threat mode in the web-based tool. The ontology browse functionality allows for all entities associated with selected controlled vocabulary terms or a combination of terms to be found. Thus, in the Threat-centric mode, the ontology search allows an end user to find all threats associated with selected controlled vocabulary or a combination of terms.

8.3.2 TRAO Ontology-Based Search

This section discusses the importance of an ontology-based search engine and different types of searches which can be carried out using the TRAO search engine are presented.

1. **Searching for an entity using property search:** Controlled vocabulary (property terms) are used to characterise terms/entities in the TRAO. For EGov Services, these terms describe among other terms, types of services, components of a service, the stakeholder involved in the delivery or reception of a service etc. A set of calculated properties which are presented as ranges are used to further characterise each term/entity. Searches based on properties that exist within the ontology allows for a controlled vocabulary of terms associated with a particular entity that is entered. Searches for properties used within the ontology are carried out using the ontology browser. These properties are displayed as a list and every relationship to these properties is presented once a property is selected. Figure 8.7 provides a diagram showing the interface for a search based on object properties. Furthermore, searches can be made on Stakeholders, Risk module, IT Service module, Asset module etc.

All Objectproperties (116)

- accessesNetwork
- addressesThreat
- affectsSecurityAttribute
- backsUp
- backsUpEGovService
- backsUpServiceProvider
- canBeIntegratedWith
- canBeIntegratedWithEGovService
- canBeIntegratedWithServiceProvider
- canEscalateTo
- canEvolveInto
- canTriggerVulnerability
- causesThreat
- compromisesAsset
- compromisesSecurityAttribute
- containsRecordsOf
- controls
- controlsData
- dependsOn
- dependsOnAsset
- enablesEGovService
- evolvesWith
- exploitsVulnerability
- exposesAsset
- hasDisastrousImpact
- hasDuplicateAsset
- hasDuplicateEGovService
- hasEffectOn
- hasLikelihoodOfVulnerabilityExploit
- hasPerformance
- hasRiskImpact
- hasRole

Figure 8. 7: Diagram showing Object Property Searches

Figure 8.8 provides an overview of an object property (addressesThreat) showing the relationships it has within the ontology. From the image, the domain is Countermeasure and the range is Threat. The hyperlinks can be used to navigate to other properties or entities within the ontology to provide more detail about.

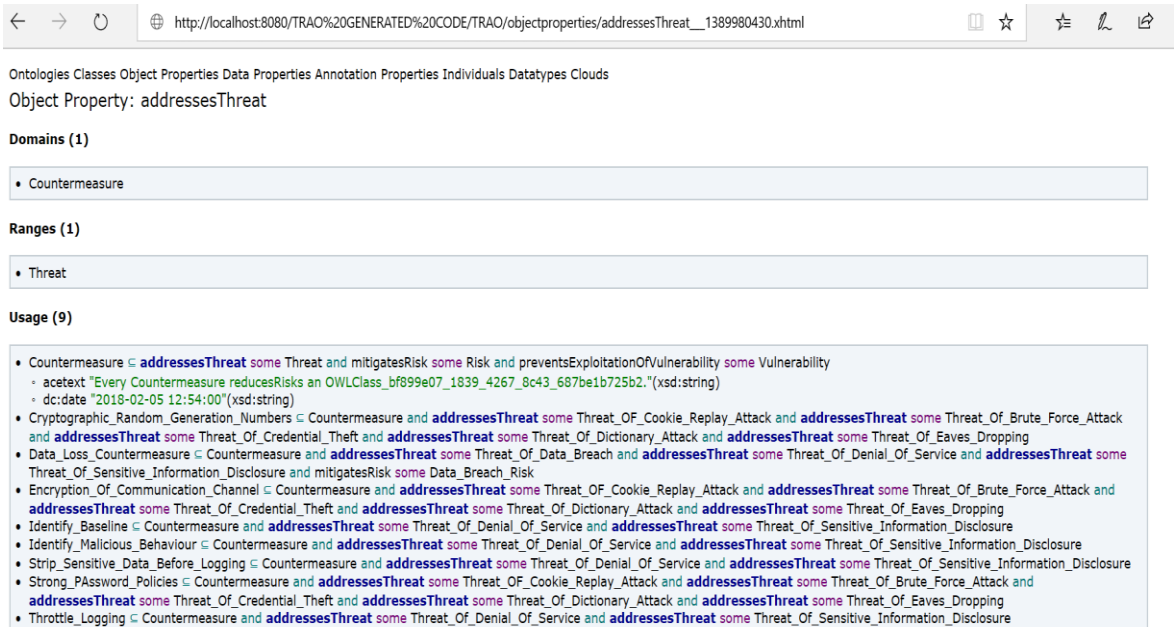


Figure 8. 8: Object Property Relationship between Two Entities

2. Performing searches using keywords

The performance of searches using keywords in the tool is made possible because they are defined in the ontology. Rahman (2013) defines a keyword as any word that is found on a web page. The use of keywords which is exported in HTML format from the ontology identifies specific records that exist within the ontology. Thus, the TRAO search facility allows terms that appear to be significant to be pulled out and indexed from the ontology.

However, although performing basic searches is required in the tool, this is not a very intelligent facility if the search engine does not consider the semantics of data represented in the ontology. Thus, the intent of the searcher and the contextual meaning in which a term or keyword is being searched had to be taken into consideration when developing the search facility of the tool so that results relevant to searches and the queries could be returned

Figure 8.9 provides a basic keyword search on the Health Service department which shows a subset of the relationship that exists between the Health Service department and other Stakeholders.

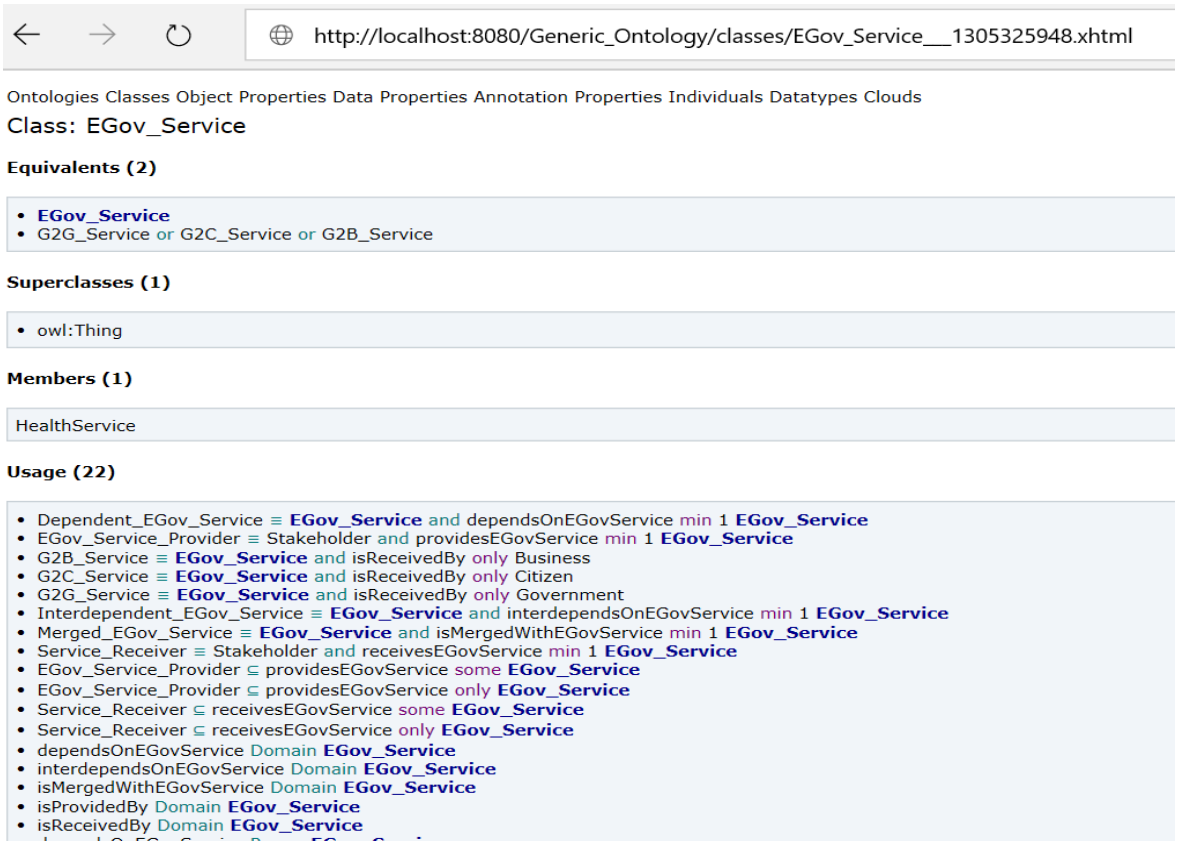


Figure 8. 9: Overview of a Search Performed on the Department of Health

3. Performing Searches using text strings

The use of a web-based browsing interface allows searches to be made on an ontology with the use of associated metadata and text strings. This form of search is more applicable using the ontology-based search engine.

8.3.3 Query Engine of TRAO

The query engine of TRAO is developed as a subsystem of the web-based Ontology Search engine described in Section 8.2.1. This feature enables searches to be made on the ontology based on the queries of a user and is made possible because the searches are carried out on the ontology URIs. The use of the query engine allows a user to type several keywords and the OWL ontology URIs are returned where the typed keywords appeared.

The queries performed needed to provide accurate results so that decision makers can know as much as possible about the results of the queries before arriving at decisions. More important to this research is that the knowledge returned from these queries need to be relevant to decision making in government in the area of evolution. To narrow the kind of queries performed, vertical searches which is a form of web search that restricts the search to the domain of discourse was employed over Enterprise search which involves a search associated with different sources such as databases, file systems, emails, document management systems, intranets etc (Rahman, 2013).

8.3.4 Development and Generation of Queries

The use of the ontology search tool allows for the easy development of queries. Queries in the TRAO web-based tool are developed based on the following steps:

1. Select the term/entity to be queried

This involves the selection of a particular term/entity using the drop-down menu. This can be referred to as performing simple searches. Users are able to search and view information provided for TRAO terms.

2. Selecting the search term

Based on the search item that has been selected for querying, more complex queries can be developed using advanced search. This allows users to apply a combination of Boolean operators (AND, NOT, OR) to obtain results to their queries.

8.4 Using Natural Language to Query the Ontology using the TRAO Query Engine

The TRAO web-based tool allows a user to formulate a query using a query engine. The query engine is divided into two panes. The query pane and the result pane. The ontology indexer allows synonyms to be matched accordingly. Thus, if a concept does not exist in the ontology, then there will no matching synonyms and then an invalid query result will be returned. The validity of a query is made possible because of the use of the reasoners in the ontology which exist and are verified on the server side. If a query is valid, the results of the query are returned. Thus, only logically valid expressions and queries are allowed by the tool. The results of the query are presented in table formats to aid a user's interpretation of the results.

Forms were developed to generate input from users. Forms were created with JSF using the technology of HTML. The forms consist of checkboxes, radio boxes and list boxes. This was done this way to accommodate different preference of users. Different queries were run using the interface and this section provides the queries and the results produced.

8.4.1 Querying the Tool Based on Scenarios in the Ontology

This section shows the way the query aspect of the tool is used. This scenario is aimed at using TRAO Web based tool for semantic querying over TRAO. Loading TRAO involved populating the TRAO web-based tool. The query engine allows for complex queries using the conjunctive (AND) and disjunctive (NOT).

In this scenario, a user is interested in knowing what stakeholders are involved with the Health Service. An image of the natural language query and results of the query are presented in Figure 8.10.

TRAO Query Engine

Question : what stakeholders are involved in Health Service

Submit

Query Result

StakeHolder Type	StakeHolder ID	Email
Service Provider	SP01	SP@de.com
Asset Manager	AM02	AM@de.com
Risk Manager	RM03	RM@de.com
Third Party Service Provider	TP04	TP@de.com
Dependent Service Provider	DP06	DP@de.com
Supporting Service Provider	SSP08	SSP@de.com

Figure 8. 10: NLI Query on Stakeholders Associated with the Health Service

Figure 8.11 shows a query to illustrate the asset components that make up the National Infrastructure and the risks they are exposed to

TRAO Query Engine

Question : what asset components make up the National Infrastructure System and what risks are they exposed to

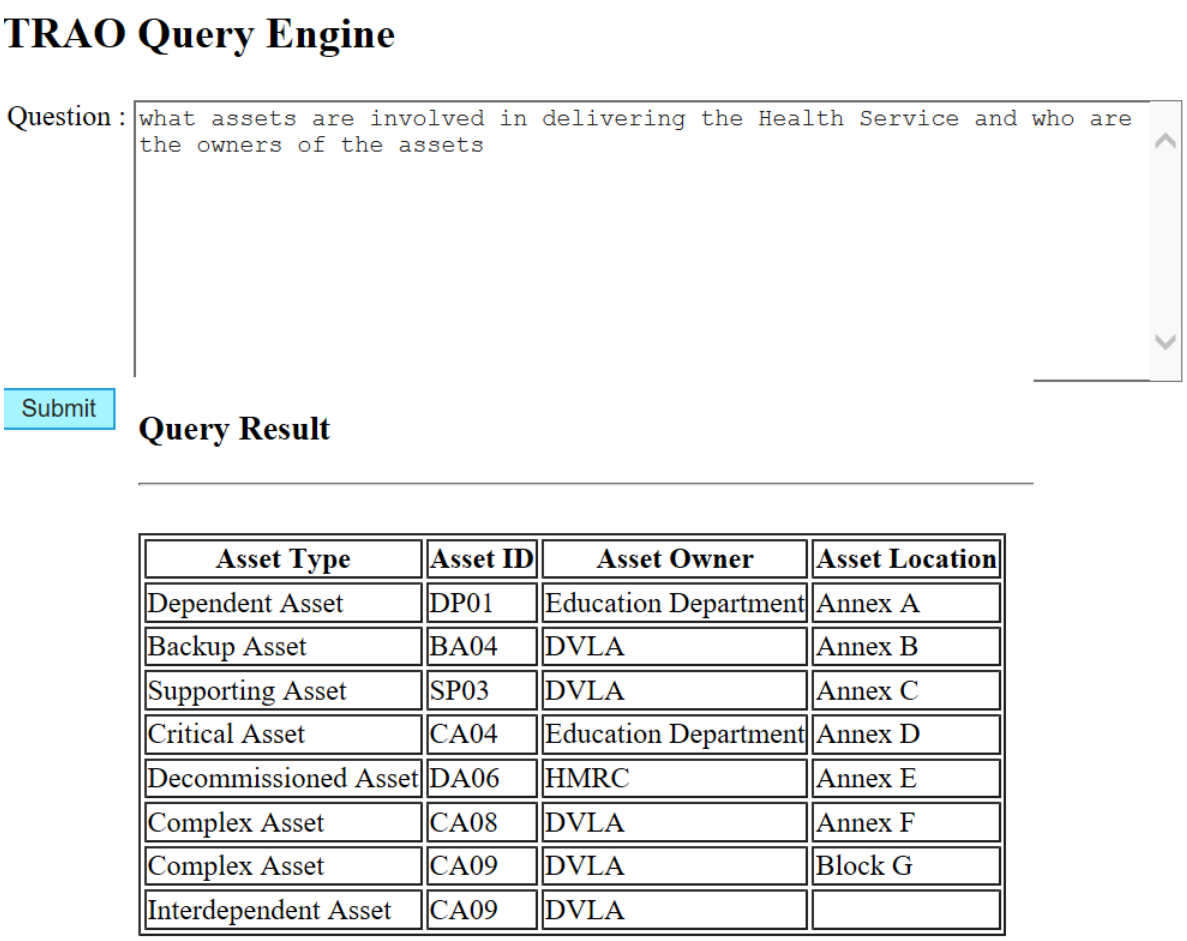
Submit

Query Result

Asset Component Type	Asset Component ID	Risk
Customer_Information_System_Payment_Infrastructure	CSP002	Failure Risk
System 1	SYS02	Disk Failure
Operating System	0S3	Operating System Failure
Data Files	DF04	Risk of Fire
National Insurance Recording System	SYS004	Risk of Decommission
OSSSystem	SYS08	Risk of Decommission

Figure 8. 11: NLI Query on Asset Components that make up the National Infrastructure

Figure 8.12 shows a query to illustrate the assets required for the delivery of the Health Service and the owners of the assets. However, the asset location is also displayed because of the rules within TRAO that attach asset owners to their locations.



TRAO Query Engine

Question : what assets are involved in delivering the Health Service and who are the owners of the assets

Submit

Query Result

Asset Type	Asset ID	Asset Owner	Asset Location
Dependent Asset	DP01	Education Department	Annex A
Backup Asset	BA04	DVLA	Annex B
Supporting Asset	SP03	DVLA	Annex C
Critical Asset	CA04	Education Department	Annex D
Decommissioned Asset	DA06	HMRC	Annex E
Complex Asset	CA08	DVLA	Annex F
Complex Asset	CA09	DVLA	Block G
Interdependent Asset	CA09	DVLA	

Figure 8. 12: NLI Query to show Assets and Asset Owners

This scenario shows a case where a word that is not represented in the ontology was used in the query. Thus, a result of malformed query was returned as there were no matches for the word *'degrade'* in the ontology.

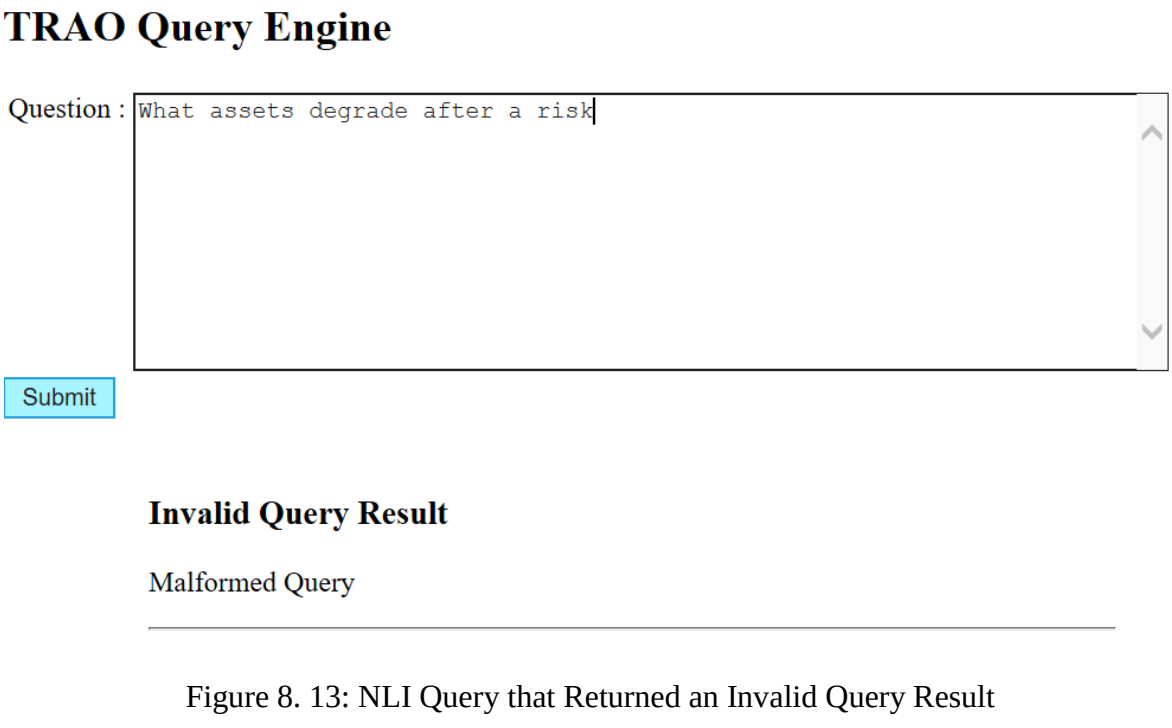


Figure 8. 13: NLI Query that Returned an Invalid Query Result

8.5 Conclusion

The results of TRAO developed in Chapter 7 are evaluated against the TRAO web-based tool which was developed in this chapter. The ontology cannot be evaluated alone given that end users do not have the required query language knowledge to evaluate it. This is a major reason for developing the web-based tool so that the whole system consisting of TRAO and the scenarios which they are applied to can be evaluated. The TRAO web-based tool enables the creation of simple but powerful queries using a NLI. The results of the queries included class and subsumption inferences which were made possible by the definition of rules in TRAO and the use of necessary and sufficient conditions. Furthermore, this chapter has further answered RQ3, RQ5 and RQ6.

"…What I mean (and everybody else means) by the word 'quality' cannot be broken down into subjects and predicates. This is not because Quality is so mysterious but because Quality is so simple, immediate and direct".

- **Pirsig (1974)**

Chapter 9: Evaluation of Ontology and Tool

This chapter discusses the evaluation of TRAO which was designed and implemented in chapter 7 and the corresponding TRAO tool which was designed and implemented in Chapter 8. While the evaluation of the ontology is based on a combination of several criteria which are discussed in Section 9.4, the evaluation of the TRAO tool is based on its functionality, usability and coverage which is discussed in Section 9.5.

The results obtained from the evaluation of the ontology are used to appraise the performance of the web-based tool as well as the conceptual framework presented in Chapter 6. This is done to determine whether the proposed usefulness and benefit of the ontology and corresponding tool are achieved. Thus, the same set of scenarios applied in the development of the ontology are run against the tool to evaluate its usefulness.

9.1 Evaluation of Research

The reason for carrying out evaluation is to ensure that the developed ontology and tool support the objectives of the research. Thus, evaluation is discussed in this chapter to validate the solutions which were employed in answering the research questions. Evaluation for this research was carried out in four parts which involved conducting a feasibility analysis amongst government stakeholders to determine the need for an ontology and a prototype tool; the second involved conducting a feasibility analysis amongst Third-Party stakeholders to determine the need for their continuous support of government services using an ontology-based tool; the third part of the evaluation involved the evaluation of the developed ontology against a given set of criteria and finally the evaluation of the prototype tool in a real world setting.

This evaluation was successfully achieved with the use of a variety of research strategies discussed in Section 5.5 and included the use of interviews which was used to establish the unique perspective of stakeholders on the subject of evolution in E-Government. This further progressed to the use of in-depth interviews. The use of in-depth interviews provided more insight and opportunities for discourse which served as a basis for the development of a combination of case studies and scenarios as modelled in Chapter 7. Furthermore, the choice of a phenomenological strategy was employed considering that the research did not limit stakeholders in sharing their personal perspectives on the subject area. The development of

the artefact used in this research went through refinement so that an appropriate model could be developed for the subject area.

9.2 Feasibility Analysis Evaluation Amongst Government Stakeholders

The feasibility analysis evaluation involved seeking audience with key stakeholders in E-Government. This involved initial correspondence using emails. The use of an interpretive phenomenological strategy guided the research design with a focus on stakeholders' meaning and understanding of the subject of evolution in E-Government. One of the reasons for the use of email correspondence was that it was a viable tool over initial face-to-face interviews given the time it took to establish contacts with stakeholders. Secondly, it provided the opportunity to develop a rapport with stakeholders.

As soon as a rapport was established, several meetings with Executive Directors of the Government Digital Service (GDS) Department in the UK were scheduled. These meetings involved approaching the Government Digital Service (GDS) Department and the Institute for Government in the UK with a short description of the research as well as a presentation on the ability of an ontology in managing complex relationships.

Objectives for these meetings were defined which involved establishing an understanding on the risk management processes in use within government, establishing a thorough understanding of the concept of evolution of services and the impacts evolution could have on assets etc. The areas of evolution discussed included the merging of EGov Services, reasons why the NPfIT failed as well as the risks associated with its failure. A positive approach to this method of asset and risk management was received and this paved the way for a second meeting. These meetings were also scheduled to determine the usefulness of an ontological-approach to managing risks in E-Government. This involved discussions on the uniqueness of the ontological approach over the traditional risk methods that are currently in use in government. Discussions at this point also revealed the need for a focus on value addition as opposed to just cost implications.

The second meeting highlighted the need for IT Services to be included in the E-Government domain considering that there is a lot of ambiguity relating to the terms E-Service, IT Service, Government Service. It was further discussed that a reason for the lack of reuse of previously developed government ontologies could be attributed to the lack of consultation with stakeholders. Also, in order for this ontology to be used, some modifications were

needed and several modifications were discussed during the meetings. A key discussion on the subject of modification involved the inclusion of an IT Service module in the ontology. Thus, this necessitated the development of the IT Service module discussed in Chapter 3. The issues raised in relation to an IT Service module are covered by the approach taken in the research design and this is shown in Section 6.2.1, 6.3, 6.4.1 and 7.5.2.

Furthermore, some of the meetings revealed the rigidity in previously developed E-Government ontologies. Some of the ontologies had actual weaknesses such as not being developed in modular form, great variation in the quality of developed ontologies, not being easy to understand for the non-expert and the use of terms that were not relatable. This further heightened the need to develop a modular ontology as well as incorporate the use of terms that were in plain English which could be easier to interpret just by merely looking at it. The development of TRAO was not without a wider consideration for the quality, content and methodology used. These were all considered to ensure that TRAO represents aspects of government in the real world and that an evolutionary path towards the development and improvement of ontologies in government is created.

The inclusion of the IT Service module in the ontology was well received by some more stakeholders as it was believed that the missing link between EGov Services and IT services had been established. Thus, the most important result of the evaluation at this stage is that the evaluation provided a proof for the inclusion of IT Services in the research approach implemented in the development of TRAO.A conclusion reached during this stage based on the experience of interacting with stakeholders is that *"until people are affected by what you do personally and what value this brings, it will continue to be an arduous task to reach out to them".*

As the meetings progressed, questions relating to the role Third-Party SPs play in government were also asked. Some of the questions involved asking if they knew how Third-Party SPs managed risks relating to government and what role government played in the management of these risks. Discussions revealed that most of their concerns in relation to Third-Party SPs were focussed on the aspect of service disruption for SRs. Thus, the key findings of the meetings with stakeholders in government are summarised in Table 9.1.

Table 9. 1: Summary of Key Findings from Feasibility Analysis with Government Stakeholders

Area of Focus	Feasibility Analysis
The E-Government system	1. The E-Government system does not exist in isolation of IT Services. Dependencies exist between services offered and IT Services. Given the criticality of dependence between EGov Services, a maturity model may be useful in demonstrating the relevance of IT service dependence as well.
	2. The drivers for the efficient management of evolution risks in government are progressively shifting from a focus on cost and complexity to a focus on value. A focus on the use of an ontological approach reflects strategic opportunities that can be created using this approach. The results of the evaluation at this stage provided a proof of concept for implementing the research approach on TRAO.
Approach to the management of risks within government	1. Evolution risks are on the increase in government. At the moment there is no centralised tool that assists stakeholders in government in knowing what assets are in use or out of use; when it is safe to say services can be merged etc. There is still a significant reliance at the departmental level which could lead to service disruption and maybe regulatory breaches in the future. The results of the evaluative study provided a proof for the development of TRAO and its corresponding web-based tool and further revealed its usability compared to existing risk management tools.
Approach to the management of Third-	1. Management of Third-Party risks are currently being looked at. However, a key concern for stakeholders in government was the disruption of EGov Services and what impact this had on the reputation of government.

Area of Focus	Feasibility Analysis
Party risks within government	2. There's a recognition of the need for more organisational awareness and commitment to the issue of Third-Party risks created by reliance of EGov Services on Third-Party SPs. The results of the evaluation at this stage revealed the extended capability of the ontology and tool to manage third-party related risks
Relationship with Third-Party SPs	1. A means for governments to identify Third-Party risks within government may be a way of committing governments to the management of Third-Party risks. This could provide a means to monitor Third-Party activities which are used in government and could significantly reduce risks created by reliance on third-parties. The results of the evaluation at this stage revealed the extended capability of the ontology and tool to assist governments in the management of third-party related risks
Use of ontological models and platforms	1. Existing or discontinued E-Government ontology models were considered inadequate and rigid.
	2. More collaboration could be encouraged between government and researchers in the aspect of developing ontological models for governments. The results of the evaluation at this stage proved the developed ontology and tool usable considering that reactions were positively received.

9.3 Feasibility Analysis Evaluation using Third-Party Service Provider

This evaluation involved making contacts with Third-Party SPs given that some of the UK EGov Services such as UK Pay and UK Verify rely on third parties for authentication and identification. The reason for conducting this evaluation was to enable governments as well as Third-Party SPs understand their position in relation to risks across rapidly evolving E-Governments. In addition to the reasons for conducting this feasibility analysis, the

management of Third-Party risks were considered as well as the opportunities the use of Third-Party SPs create.

General objectives were set out for these meetings and questions relating to Third-Party SPs supporting some of government services were asked. The objectives of these meetings included: identifying if Third-Party SPs are made aware of the kind of risks associated with supporting EGov Services; if there was any form of support received from government in the management of these risks; if they had an internal risk management model and what type of model they had in use while offering Third-Party services; the difficulties they encountered with managing Third-Party risks etc.

This evaluation involved conducting a meeting with four different managers in Nationwide Building Society in Swindon, UK at different times. Nationwide Building Society was chosen because of the ease in establishing a point of contact during the research. The meeting was focussed on asking questions relating to Third-Party risks and how banks which are responsible for verifying some of the services in government are able to manage the risks associated with that especially with respect to dependence on assets.

Discussions in this area revealed some form of reliance on government systems as well as some Third-Party external SPs which this thesis refers to as Fourth Party Service Providers in order to fulfil their obligations to government. Although, there are currently risk management practices in place amongst Third-Party service providers, discussions further revealed that an ontological approach to the management of risks especially in the case where Third-Party SPs have to depend or interdepend on fourth party SPs may help in determining risks they are prone to.

As with governments, these Third-Party SPs find themselves faced with similar siloed situations. A typical case highlighted during discussions with the managers further revealed that some organisational units of Third-Party SPs were decentralised which had created inconsistencies in the approach taken to manage risks in the past.

Further discussions also revealed gaps in the current tools being used especially in the aspect of timeliness in identifying risks which thy believed could result in poor service performance which could result in regulative breaches. The use of the ontological approach was seen to be beneficial in these areas and showed how third-party risks could be identified and managed. The most important aspect of this evaluation was that it provided a

proof for the use of the ontological approach. It showed the ontological approach to be usable and predictive compared to the traditional based tools currently in use. Discussions in this area also progressed to the use of an ontological based approach in managing risks especially in the aspect of unsecured lending. However, as this was out of the scope of the research discussions relating to these were proposed for the future. Thus, the key findings of the meetings with Third-Party SPs are summarised in table 9.2.

Table 9. 2: Summary of Key Findings with Third-Party Service Providers

The Third-Party System	1. There are dependencies that exist between organisational units in Third-Party SPs. These dependencies have increased the ned to critically manage the relationships that exist between organisational units.
	2. There are dependencies that exist between Third-Party SPs and other Third-Party SPs leading to Fourth-Party SP relationships. Thus, there is the need to enhance the existent models between Third-Party and Fourth-Party SPs. The results of the evaluation carried out this stage provided a proof of concept for the management of third-party risks
Approach to the management of Third-Party risks	1. There is a paradigm shift in the approach taken considering the proposal of an ontological model and the functionality it brings. This should increase the focus on value as opposed to cost implications.
	2. Inconsistent approach used in the identification and management of risks because of existence of siloed processes. The results of the evaluation revealed that the use of an ontological based approach can significantly increase consistency across third-party SPs.
Existing platforms in use	1. The platforms and models in use may not be adequate for use in the future giving the complexity of changes that are seen to be occurring.

	2. Thoughts are being given to whether Third-Party risk management should continue to be outsourced or whether an in-house risk management tool can be used for managing third-Party risks. Reactions to the use of the web-based tool were positively received which showed avenues for wider development.

9.4 TRAO Evaluation

The task of measuring the quality of an ontology is referred to as ontology evaluation. Evaluating an ontology allows the main question regarding the development of the ontology to be answered (Vrande *et al.*, 2010). An important part of the technology of the semantic web is to be able to evaluate the quality of the classifications used in the ontology (Maynard, 2006). An ontology can have several potential uses. Thus, there is no universally defined list of requirements or approaches that is applicable for evaluating an ontology (Neuhaus *et al.*, 2013). Some of the criteria used in previous research in evaluating an ontology are presented:

i. Based on all relevant terms from documented use cases (Neuhaus *et al.*, 2013);
ii. Evaluating an ontology by themselves (Vrande *et al.*, 2010);
iii. Based on all entities used within the ontology being within the scope of the captured ontology (Neuhaus *et al.*, 2013);
iv. Natural language based evaluation which is completely based on population of the ontology and semantic metadata creation (Shah *et al.*, 2015)
v. Ontologies can be evaluated within some context (Vrande *et al.*, 2010);
vi. Application-based method of evaluating an ontology which involves evaluating an ontology within an application (Brank, Grobelnik and Mladenić, 2005);
vii. Based on a unanimous agreement reached by the domain experts on the ontological analysis (Neuhaus *et al.*, 2013);
viii. Task-based ontology evaluation which involves evaluating an ontology in the context of a task and application (Porzel and Malaka, 2004)
ix. Data driven evaluation which involves comparing the ontology to existing data (Brank, Grobelnik and Mladenić, 2005);

The evaluation of the ontology was assessed by ontology experts to establish the reasons for the development of the ontology and to ensure that TRAO captured relevant concepts and meets the requirements of the application. This evaluation also involved the use of reality as a benchmark. Although it was impossible to completely rely on reality given the unavailability of previously developed E-Government ontologies and the inability to compare TRAO against them, independent ontology experts were able to arrive at the conclusion that the concepts relating to the research and competency questions had been met by the ontology. In addition to the coverage of the ontology, it was established that the strength of TRAO can be attributed to its successful use, adoption and extension.

A variety of other methods were employed during the evaluation of the ontology. This section discusses the methods of evaluation used for the ontology. A combination of methods was used to ensure that the ontology was fit for purpose and met a variety of evaluation criteria.

1. Evaluating the ontology based on its fidelity

TRAO was evaluated based on its coverage, expressivity and appropriate representation of the domain which it passed. Neuhaus *et al.*, (2013) posits that the evaluation of an ontology based on its fidelity should focus on the classes, properties and axioms defined in the ontology. TRAO is made up of 1212 entities consisting of 844classes, 116 object properties, 210 individuals, 24 data properties, 12 annotation properties and 6 datatypes. Thus, the fidelity of the ontology was checked by identifying if TRAO matched the characteristics of the real-world description and whether it contained the relevant classes, properties and axioms. Evaluation of the ontology based on its fidelity also involved ensuring that all axioms within the ontology are true with respect to the intended level of granularity. Furthermore, this evaluation focussed on evaluating the logical consistency of the ontology and the automatically generated results from the ontology based on the interpretations provided by the reasoner. Thus, TRAO consistency checks were carried out in Protégé 4.2, 4.3 and 5.0 versions using two different reasoners (Fact ++ and Pellet). The ontology was considered consistent at the end of the evaluation as there were no inconsistencies at the end of the evaluation.

2. Evaluating the ontology based on its fitness

This involved evaluating the ontology against the set of competency questions presented in table 7.2 and against the scenarios which were developed in sections 6.6. The set of competency questions and scenarios were revisited to ensure that the ontology is able to answer the questions and can be used to prove that it supports the scenarios. The competency questions were used to query the corresponding ontology modules and the whole ontology to ensure that the right relationships between entities were established in the ontology. This form of evaluation was successful given that queries completed successfully which was proof to show that the model requirements of the ontology were adequately met.

3. Evaluating the ontology based on its appearance on the web

The basic appearance of the ontology on the web was also used in the evaluation of the ontology. A correctly developed and consistent ontology should be correctly represented on the web through parsers (W3C, 2004). Thus, the web representation of the ontology was inspected using a white box testing to determine whether the underlying logic behind its development behaves correctly. The coding of the ontology was compared with links in the web representation to evaluate if the representations and the inferences generated from the ontology were consistent. Figure 9.1 provides an overview of the web representation of the ontology.

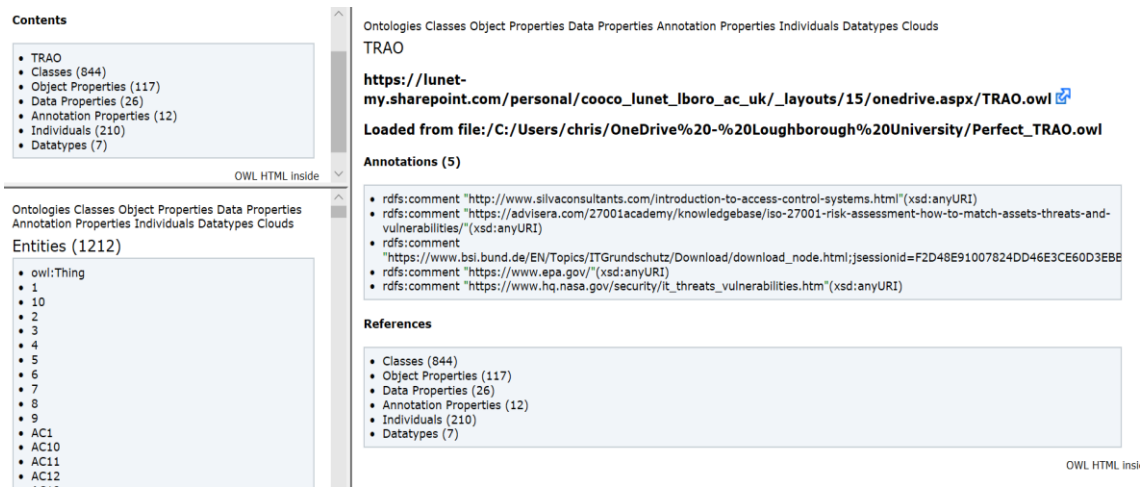


Figure 9. 1: Overview of the Web Representation of TRAO

4. Evaluating the ontology using existing tools

TRAO was also evaluated against an existing tool known as Rightfield. This was used in

adding ontology term selections to semantically aware Excel spreadsheets (Wolstencroft *et al.*, 2011). In other to evaluate TRAO in a real ontology building scenario, a template for gathering information relating to the key concepts used in the ontology have been populated. A range of allowed terms from TRAO were used to populate the spreadsheet and present them to users as simple drop-down list. A malformed ontology would not be able to be evaluated in this way. A diagram showing the representation of the ontology in Rightfield is presented in Figure 9.2 while a figure showing the conversion of Rightfield to semantically aware spreadsheets is shown in Figure 9.3.

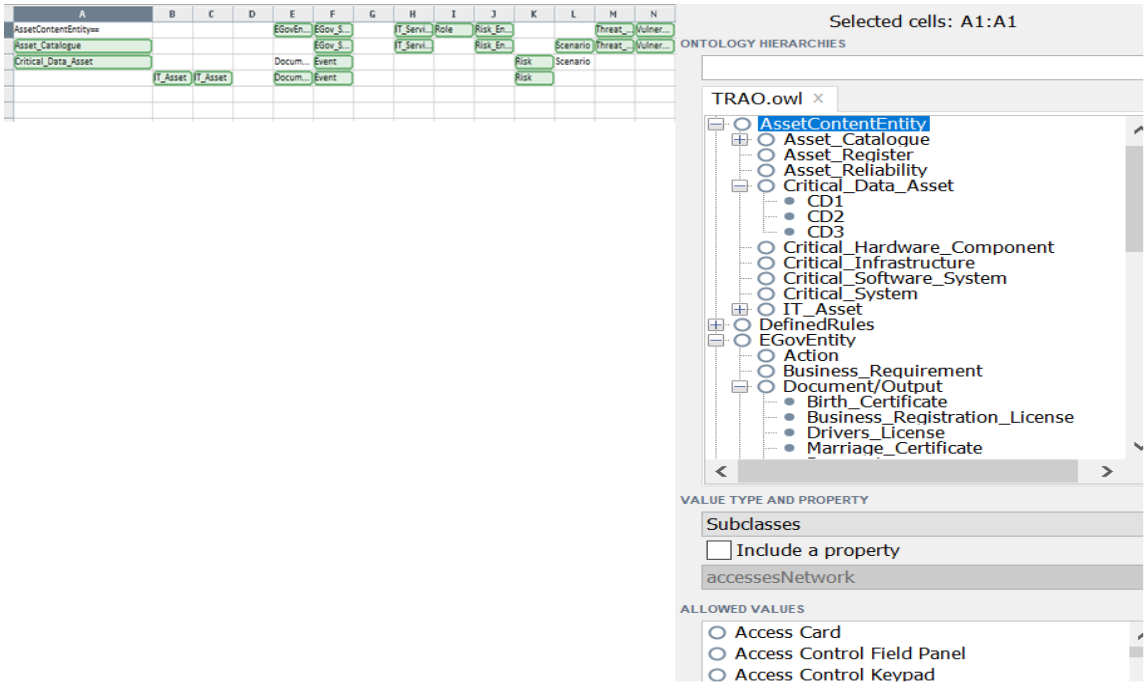


Figure 9. 2: Diagram showing Ontology in Rightfield

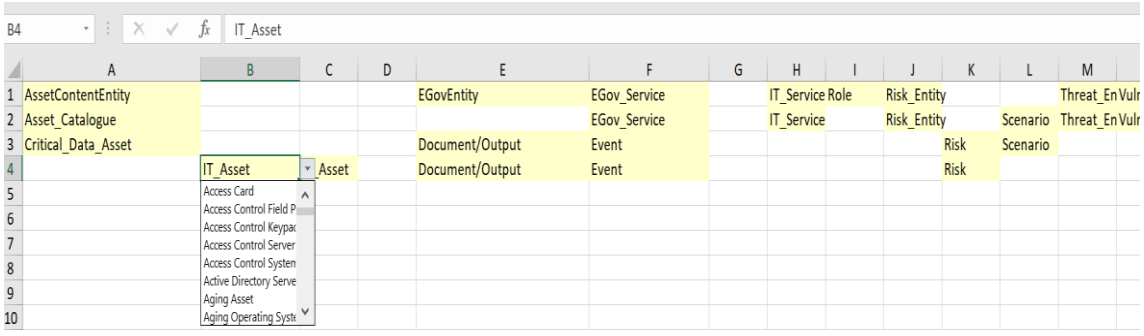


Figure 9. 3: Diagram showing Semantically Aware Spreadsheet Generated using Rightfield

9.5 Tool Evaluation

Within the E-Government domain, a variety of tools already exist which are used to manage risks in E-Government. However, discussions with stakeholders revealed that there is currently no tool that manages risks associated with evolution in E-Government. Thus, there are identified limitations in the use of the traditional based tools. This evaluation showed that the TRAO web-based tool will help in identifying the risks associated with evolution in E-Government. The evaluation of the level of usability of the TRAO tool forms part of the evaluation carried out during the research.

The evaluation of the tool was also based on some criteria which include the following:

i. Usability: this was carried out to determine the perceived usefulness of the tool in comparison with real world examples (Pressman, 2001);
ii. Coverage: the coverage was used to show the extent to which a user could query the ontology using a web-based tool
iii. Functionality: the ease of use of the tool was determined based on described functionalities of the tool as discussed in Chapter 8.

Questions were asked to evaluate the tool based on the three criteria presented above. Some of the questions are presented in Table 9.3.

Table 9. 3: Tool Evaluation Questions

S/No	Question
1.	How useful do you think the TRAO tool is to present day E-Government?
2.	Do you think the use of an ontological method is a better approach to managing risks in E-Government?
3.	Do you think this prototype tool can be adopted by governments based on its usefulness?
4.	Are there any other aspects of E-Government that an ontological approach would be beneficial?

5.	Did this tool meet your expectations? What were some of the interesting features when you interacted with it?

The evaluation of the tool involved the use of the tool by Directors of the GDS. The directors of the GDS were involved in this evaluation given that their assessment of the tool could have major transformative impacts. Also, their involvement could help in understanding future problems that could be addressed as well as provide governments with feedback on the objective view of the project; their involvement could provide further corrective actions to resolve issues that may be outstanding which could be implemented to improve the performance of the tool.

The evaluation involved the use of natural language questions within the scope of the ontology to run queries and then asking the users how satisfied they were with the results of their queries. Furthermore, a manual comparison of the results obtained from the queries with results from the ontology was carried out. Some of the queries stakeholders were interested in asking the tool include the following as shown in table 9.4.

Table 9. 4: Representative Questions used During Evaluation

S/No	**Question**
1	What assets are used by a particular EGov Service?
2	How do we know what assets are vulnerable to a particular vulnerability
3	If an ontology is susceptible to at least 5 risks, can it be reused?
4.	What are the risks involved in merging two departments?
5.	What are the risks involved in merging the systems of the Care service with the Health Service?
6.	When can an asset be said to be complex and what are the risks associated with this complexity?

The use of the natural language interface of the tool hid the ambiguity associated with the use of query languages by untrained people. The use of the ontology indexer allowed for the matching of variants of the same concept. An analysis of the detailed results of the use of the tool in answering queries showed that on all occasions, the use of the tool returned correct answers. However, there were 2 cases of incorrect answers produced by the tool. A manual analysis of the incorrect answers showed that there was no such concept represented in the ontology and therefore the ontology could not generate synonyms of the concept either. This was carried out just to test the functionality and coverage of the tool as well as its ability to be extended. The 2 cases of incorrect answers were based on the following queries:

1. What assets degrade after a risk?
2. What risks produce a greater risk impact?

Considering that the object properties of 'degrade' and 'produce" and the class 'Greater Risk impact were not included in the ontology and no matching synonyms existed, the result of invalid query result was received.

9.6 Results of the Evaluation

Three stakeholders in government and four Third-Party SPs participated in the evaluation of the research. The results of the evaluation show that there is the need for an ontological approach in the management of risks in E-Government. Furthermore, the feedback from the feasibility analysis was considered meaningful and supportive of the processes that take place in government. The results of the effectiveness of the system evaluation are presented in this section to assess the range of the questions that the TRAO system can answer. Based on the scope of the ontology, the use of the web-based tool and time constraint; a set of 28 queries were generated. An analysis of the effectiveness of the developed system is discussed in this section to assess the kind of questions the TRAO system was able to answer correctly and the degree to which the stated goals and objectives have been achieved.

The overall Effectiveness of the system was calculated based on the six criteria proposed by Cleverdon, Mills and Keen (1966) for the evaluation of an information retrieval system. Based on the six criteria, this research is interested in precision which is the ability of the system to present only those items that are relevant.

$$Precision = \frac{Number\ of\ relevant\ queries\ correctly\ answered}{Total\ number\ of\ queries} \text{ x } 100\%$$

$$\text{Precison } = \frac{26}{28} \text{ x } 100\%$$

$$\text{Precision= } 92.8\%$$

Thus, the effectiveness of the designed system was 92.8% which is a very good value that shows how effective the system is in answering queries. The 7.2% ineffective system rate is equivalent to the two cases mentioned in Section 9.5 where there were no concepts related to the ontology that were included in the query. Considering that precision depends largely on the relevance judgement of the user, it can be concluded that since the system returned more relevant results than irrelevant ones, the system can be said to be highly effective. Furthermore, based on the use of related terms and synonyms for concepts represented in the ontology, the percentage of matched/mapped terms shows that the system is highly effective.

9.7 Conclusion

This chapter discussed the different methods of evaluating the ontology and the web-based tool. Firstly, the evaluation discussed how stakeholders' perception of an ontology-based tool informed the researchers modification of the ontology. Results from the evaluation carried out in this research show that the TRAO web-based tool prototype has valuable potential to improve the practices surrounding the management of evolution risks in E-Government. Based on the overall System Effectiveness and the results of the evaluation have shown that it may be useful to build on this prototype to develop into a system that is managed centrally by government. Furthermore, this chapter has further answered RQ1, RQ2, RQ4 and RQ5.

Chapter 10: Research Conclusions, Recommendations and Future Work

This chapter summarises the findings from this research. Conclusions are reached based on the hypothesis that an ontology based-approach can be used to improve the management of evolution related-risks in the E-Government domain. The aim of the research is to analyse what happens as evolution takes place in terms of risks using an ontology-based approach. This aim has focussed on (i) assisting key stakeholders in E-Government in defining existent relationships and compositions and their effects using a web-based tool to run queries on the ontology; (ii) providing support for stakeholders in understanding where reliance on an asset should not exceed the trustworthiness of its component parts given that a component of an asset may be vulnerable to certain vulnerabilities which may have cascading impacts on an EGov Service. The findings, results, limitations of the research, contributions and recommendations for future work are presented in this chapter.

10.1 Conclusions Reached

The use of an ontology-based tool has the potential to improve the management of risks in the E-Government domain. It also has the potential of improving the management of risks revolving around the area of evolution of EGov Services. This study has provided substantial research to show that the use of an ontological approach can greatly increase the effectiveness of government and provide a better approach on how the subject involving risk is approached in government. Furthermore, analysis of the evaluation of the tool has also shown that there is the potential for government to better manage the assets that are being used as well as understand the stakeholders who are affected by the evolution of EGov Services. Based on this reason, an overarching research question formulated for this research question was as follows:

How can governments identify assets or services that are susceptible to risks if these assets or services in governments must evolve, and what impacts does this evolution have on services?

To answer this research question, this thesis developed a conceptual framework in Chapter 6 which was aimed at understanding the risks that occur as EGov Services evolve and the effect this evolution has. A hermeneutic research strategy was employed in the identification

of important concepts for the research and logically linking them together. Thus, a framework was developed in Chapter 6 which was used to unify concepts between different domains (E-Government, Assets, IT Services, Security) by mapping these concepts into conceptual models. The framework provided a basis for the use of an integrated ontology (TRAO), an interface for querying the ontology with the use of the tool, a query module for retrieving relevant information from the ontology, a triple store module for producing a dynamic object model of the ontology and an indexer which is responsible for deriving variants of the same idea.

The development of the conceptual framework provided a basis for the development of an integrated ontology in Chapter 7 and a web-based tool in Chapter 8. This framework was then refined in Chapter 8 and used to analyse different scenarios and two interpretive case studies that took place between the GDS and a Third-Party SP. A feasibility analysis of the web-based tool provided meaningful feedback and lessons on how risks can be better managed in E-Government and even amongst Third-Party SPs given the level of evolution that is on the increase. Furthermore, the feasibility analysis conducted with the GDS provided reasons for the modification of the initially developed ontology to include an IT Service module. Thus, the developed 5-level E-Government model in Figure 6.1 was extended to include the IT Service layer. A novel contribution of the web-based tool is the use of variants of the same idea during querying. Thus, synonyms of concepts that exist in the ontology were retrievable if a related concept was used during the querying.

10.2 Research Questions Revisited

The individual research questions and the sub questions presented in Section 1.2 are revisited and answered in Table 10.1. Given the number of sub questions, a set of questions are answered as proof that the research has addressed all the questions.

Table 10. 1: Research Questions Revisited

	Research Question	**Summary of Answer**
1	Who owns a service and who is responsible for its management?	It has been established in Chapters 1, 2 and 3 that a provider of a particular EGov Service is the owner of that service. Chapter 7 provides a model for this relationship to show that EGov Services are provided by SPs and the feasibility analysis conducted in Chapter 9 support such claims from literature.
	What assets does a service require to run on?	Sections 2.4.1 provided an analysis on the effects of redesign and it was established in the literature that before a service can be redesigned, the assets it runs on must be analysed. Furthermore, Section 3.3 also discusses EGov Services in relation first to IT Services and then to IT assets. The conceptual framework in chapter 6 support this claim that an EGov Service cannot run on its own without assets. Furthermore, the feasibility analysis in Chapter 9 also support the conceptual framework and the evaluation of the tool provide meaningful results to show this.
	Does a service require more than one asset to be in place?	Table 3.2 provides the application of SOA principles in this thesis. The principle of composability shows that an asset can be composed of asset components which are also assets. It has also been established based on the use of the hasPart relationship (7.5.3) and the principle of transitivity applied in the modelling of the ontology (6.5.3) that If an EGov Service requires 1 asset, it invariably requires that asset and its component parts to be able to run.

	Research Question	Summary of Answer
2	What are the risks associated with vulnerable assets?	As established in literature, there is often a mix up between the concepts of risk, vulnerability and threat. Chapter 6 provided a conceptual model to describe the relationship that exists between the vulnerability and asset class. It also established a relationship between the concept of vulnerability and risk. The measurement of the risks associated with vulnerable assets is modelled based on the gaps and weaknesses that can be exploited by a threat. Thus, the literature in Chapter 3 provides a basis for the conceptual model in Chapter 6 and the ontological model in Chapter 7 shows the relationships between Assets, vulnerability and risks.
	How vulnerable are assets that are dependent?	Literature on assets and vulnerability has established that not all assets are created equal and therefore, there are some assets that are more critical to the operations of government. Literature in Chapters 1, 2 and 3 provided a basis for modelling dependencies that exist between assets in the conceptual framework in Chapter 6 and the ontology in Chapter 7. It has been established that an asset may depend on another asset. Considering the SOA principle of composability and the rules specified in the ontology, vulnerabilities can cascade and an asset component may be vulnerable to the vulnerabilities of the asset. The evaluation of the tool in Chapter 9 provided results on this.
	What are the risks associated with dependencies of single/complex systems, components or infrastructures?	As with the issue of vulnerability, risks can cascade from Assets to its component parts. Thus, the component parts of an asset are exposed to those risks. The framework provided insight on this as well as the evaluation of the ontology and tool in Section 7.6.4, 7.6.7.

	Research Question	Summary of Answer
	What kind of risks occur if a service or system is decommissioned?	Decommissioning was addressed in Chapter 1 as one of the reasons for evolution. Section 7.5.3 models a decommissioned asset as one with a Decommissioned state and associated risks are presented on this.
3	How can the complexity of multiple dependent assets be managed?	The use of the ontology provides a basis for the management of dependent and complex assets. This is addressed in Sections 6.3.3, 6.3.7, 7.5.3.4, ad 8.4 Furthermore, the use of the ontology-based tool is able to provide results on complex assets as well as assets that are in the category of complex and dependent. The developed framework and ontology are flexible enough to allow modifications based on the complexity, structure and available resources of organisations. Furthermore, feedback from the feasibility analysis shows that the management of complex assets poses great challenges and the incorporation of an audit function in the tool may help with managing this category of assets. However, this was beyond the scope of the research.
4	How prepared are governments in the management of evolution-related risks?	In terms of risk management, governments are making use of tools to manage their risks. However, it was obvious from the evaluation that governments still need to think long term and forecast to enable them strategically to prepare for evolution-related risks. The feasibility analysis in Section 9.2 provided results on this. A better understanding needs to spiral down as well to government stakeholders on the complex nature of government so that they can become more aware of the rising interconnectedness that exists in the E-Government domain.

	Research Question	Summary of Answer
5	Can a model from the ontology be developed from the results of the research and applied to government systems?	A model from the ontology can be developed and reused across governments based on different queries that can be accommodated by the TRAO web-based tool. This is also possible because of the interface that exists between the ontology and search requests which provide result sets that are as close as possible to the user's natural language query. The development of the ontology, corresponding web-based tool and the evaluation using real world examples has created more opportunities for standardization in the E-Government domain. This is because TRAO has also provided a means to facilitate integrative analysis over heterogenous data in different research fields. This is evident in the development of the ontology in Chapter 7, the corresponding tool in Chapter 8 and the evaluation of the use of the ontology and tool in Chapter 9
6	Does TRAO demonstrate how much change a system can accommodate?	The ontology is able to model services and departments that can be used as backup in cases of failure. Rules specified in the ontology show that a system can be used as a backup for another system if they have at least 4 similar critical components. Thus, the issue of having backups in the case of failure or decommissioning is accommodated in the ontology. This is addressed in Sections 7.8 and 7.9.
	Does the ontology show the risks associated with reuse of service components and infrastructures?	The ontology accommodates different types of risks and the development of the ontology was carefully considered based on the different competency questions. Thus, the ontology models the risks

	Research Question	Summary of Answer
	Can the ontology be used to show the risks associated with resource sharing?	associated with reuse of service components and infrastructures as well as the risks associated with sharing of resources.
	Can the ontology be used to calculate the probability of risks occurring in a government or the probability of a system being vulnerable?	The ontology is able to calculate the probability of risks. Given that the issue of forecasting and prediction came up during the feasibility analysis with stakeholders, providing this functionality through a set of rules in the ontology was accommodated. This was modelled in the ontology based on establishing a link between probability of failure to the age of an asset and linking the probability of failure to direct observation tables as presented in Section 7.5.3.4.

Considering that the overarching research question which was broken down into RQ1-RQ6 have been answered; this thesis is considered to be complete.

10.3 Considerations for Future Work

The developed framework, ontology and tool have proven to be a valuable tool for managing evolution risks in E-Government. However, in the course of answering the research questions, the interest in this research area is not exhausted and a number of areas for future research have been identified. Some areas of consideration for future work are presented in this section.

a) Feedback from the Third-Party SPs also revealed the need for an ontological approach in the management of risks amongst Third-Party SPs. It will be useful to expand the scope of this research to incorporate this.

b) The research within this thesis has been specific to governments, it would be interesting to see how this approach can be applied in other domains.
c) More research is required to investigate the existent best practice risk methods that are applied in government and how this can be compared against the new TRAO model
d) It will be interesting to carry out an analysis on assets maintaining different states within the ontology considering that all assets were assumed to maintain the same state.

10.4 Research Contributions

In the words of Robin Sharma *"Success is not a function of the size of your title but the richness of your contribution".* This section revisits and provides full details of the contributions made by this thesis as summarised in Chapter 1. The overall purpose of the research as stated earlier has been to analyse the risks associated with evolution in E-Government using an ontology-based approach. To the best of this researcher's knowledge, peer-reviewed published papers; prior to this thesis, an ontological based-approach to the identification and management of evolution risks in E-Government did not exist. The contributions of this thesis are:

a) The development of the conceptual framework in Chapter 6 which is based on the theoretical foundation of the main aspects of the research. This was conducted based on hermeneutic literature reviews;
b) The development of individual conceptual models for the areas of discourse and a unified conceptual model. This is presented in Chapter 6;
c) The development of an ontological-based approach that analyses what happens as assets (component, systems, platforms, infrastructures) continuously evolve in terms of risks and vulnerabilities using an ontology. The results of this are presented in Chapter 7;
d) The development of a tool to interface with the ontology in Chapter 8 which allows for natural language queries.
e) The use of a case study which was formulated with the help of scenarios which were developed in Chapter 7 and applied in Chapter 9.

f) A method to analyse the risks associated with evolution in E-Government. This is seen as the primary contribution of this research. This contribution combines the evaluations of the ontology and the tool in Chapter 9.

Three additional papers are in progress resulting from the work carried out in this thesis. The first is concerned with the presentation of the approach used in modelling the ontology. The second is concerned with the development of the web-based tool and its ability to run natural language queries while the last paper is on the developed framework for the analysis of evolving risks in the E-Government domain.

10.5 Research Limitation

Although the aims and objectives of the research have been established, there were some limitations that existed during the research. A major limitation was the difficulty in getting stakeholders in government to evaluate the research. A lot of time was spent trying to get key stakeholders to evaluate and provide feedback on the proposal which had knock on effects on the time left to complete the research.

Given the difficulty in getting stakeholders to evaluate the research, the evaluation of the research was limited to only two sets of stakeholders (Service Provider and Third-Party SP. There is the possibility that the applicability of the conclusions obtained from the evaluation cannot be generalised. Although care was taken while making generalisations in this research, having a wider range of stakeholders to evaluate the research at different levels would have provided larger generalisations for a wider range of government.

A third limitation which had major impacts on the research was time. It took almost 2 years to get the stakeholders that evaluated the research. Despite repeated emails and referrals, government was very closed in their response. Thus, interaction which should have been established at the onset of the research was not established. Therefore, more time was spent on the development of the ontology and tool instead of following the sequence of exploring the problem first, then developing a design. Thus, this led to the re-development of a layer of the already developed ontology and tool.

10.6 Closure

In conclusion, this research has provided a lot of experience and insights into the aspect of risk management in E-Government and the role technological evolution plays in the evolution of EGov Services and assets. This research has been very enlightening and finally a real evidence of a conceptual framework, ontology and tool now exist for the domain of discourse. The approach used in this thesis and the development of these artefacts is the beginning of what is hoped will be the beginning of a better and more suitable approach to the continuous management of risks in E-Government.

References

Abbott, C., 2017. Gov Design. Making it easier to book meeting rooms. Available at: https://dwpdigital.blog.gov.uk/author/craig-abbott/

Accenture, 2017. Redesigning the Back Office for Government Transformation. Available at: https://www.accenture.com/gb-en/insight-redesigning-back-office-government-transformation.

Adewunmi, A., 2015. Making data a public asset through infrastructure. Available at: https://gds.blog.gov.uk/2015/11/03/making-data-a-public-asset-through-infrastructure/ [Accessed May 18, 2017].

AECT, 2001. Qualitative Research Methods. introduction to qualitative research. Available at: http://members.aect.org/edtech/ed1/40/40-01.html

Agarwal, R., C., H. & Lucas, J., 2005. The Information Systems Identify Crisis: Focusing on HighVisibility and High-Impact Research. *MIS Quarterly*, 29(3), pp.381–398.

Agile delivery community, 2016. Agile and government services: an introduction. Available at: https://www.gov.uk/service-manual/agile-delivery/agile-government-services-introduction [Accessed July 22, 2017].

Agrasala, V., 2011a. External, Internal and Support Services – A welcome addition to ITIL 2011. Available at: https://vagrasala.wordpress.com/2011/09/02/external-internal-and-support-services-a-welcome-addition-to-itil-2011/.

Agrasala, V., 2011b. What is IT Service? Available at: https://vagrasala.wordpress.com/2011/12/06/what-is-it-service/.

Aikins, S.K., 2014. A Risk-Based Audit Model for Improving the Success Rates of e-Government Project Implementation. In *Public Administration in the Digital Age*. p. 15.

Aime, M.D. & Guasconi, F., 2010. Enhanced vulnerability ontology for information risk assessment and dependability management. *Proceedings - 3rd International Conference on Dependability, DEPEND 2010*, pp.92–97.

Airey, E., 2015. IT modernization strategy: Reuse rather than replace. Available at: https://gcn.com/articles/2015/03/18/cobol-modernization.aspx.

Aked, M., 2003. *Risk-based planning with use cases*, Available at: www.lamri.com.

Alasem, A., 2009. An Overview of e-Government Metadata Standards and Initiatives based on Dublin Core. *Electronic Journal of E-Government*, 7(1), pp.1–10.

Alazemi, N. N., Al-Shehab, A. J. and Alhakem, H. A. (2017) 'E-government Frameworks based on Semantic Web Services: A Comprehensive Study', *International Journal of Computer Applications*, 158(7), pp. 975–8887. Available at: http://www.ijcaonline.org/archives/volume158/number7/alazemi-2017-ijca-912848.pdf.

Albert, R., Albert, I. & Nakarado, G.L., 2004. Structural vulnerability of the North American power grid. *Phys. Rev. E*, 69, p.art. no. 025103.

Albert, R., Jeong, H. & Barabasi, A.-L., 2000. Error and Attack Tolerance of Complex Networks. *Nature*, 406(July), pp.378–381. Available at: http://www.nature.com/doifinder/10.1038/35019019.

Aldrich, D., Bertot, J.C. & McClure, C.R., 2002. E-government: Initiatives, developments, and issues. *Government Information Quarterly*, 19(4), pp.349–355.

Al-Khatib, H., 2009. A Citizen Oriented E-government Maturity Model. , pp.1–14.

ALSoud, A.R. & Nakata, K., 2011. A Conceptual Life Event Framework for Government-to-Citizen Electronic Services Provision. , pp.1–10.

Altexsoft, 2017. Legacy System Modernization: How to Transform the Enterprise for Digital Future 1. , pp.1–20.

Alvaro, A. *et al.* 2007 'C . R . U . I . S . E : Component Reuse in Software Engineering'.

Andrews, E. et al., 2016. *Making a success of digital government*

Anne M. Cregan, 2008. Chapter I. Overview of Semantic Technologies. In *Handbook of Ontologies for Business Interaction by Peter Rittgen*. pp. 1–20.

Anthopoulos, L.G. & Manos, A.D., 2005. e-Government beyond e-Administration . The Evolution of Municipal Area Environments Could Establish a Digital ... Framework of Confidence for Citizens. , (January 2005).

Arango, G. & Prieto-DiazG., R., 1989. Domain Analysis: Acquisition of Reusable Information for Software Construction. *IEEE Computer Society Press*.

Arkin Software Technologies, 2016. Legacy Modernization – Transformation into an Agile Enterprise.

Arogundade, O.T., Jin, Z. & Yang, X.G., 2011. Enhancing Use Cases with Subjective Risk Assessment. *2011 Fifth International Conference on Secure Software Integration and Reliability Improvement - Companion*, pp.144–151. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6004516.

Arroyo, S. & Siorpaes, K., 2014. Ontologies and Ontology Languages. In *Handbook of Metadata, Semantics and Ontologies2*.

AS / NZS ISO 31000, 2009. Risk Management- Principles and Guidelines.

Asa'd M. As'ad et al., 2017. Importance of service integration in e-government implementations.

Asia Pacific Fraud Survey, 2013. Knowing your third party. Available at: http://www.ey.com/Publication/vwLUAssets/EY-Knowing-your-third-party/$FILE/EY-Knowing-your-third-party.pdf.

Australian National Audit Office, 2000. Electronic Service Delivery , including Internet Use , by Commonwealth Government Agencies. , (18).

Avižienis, A. et al., 2004. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1), pp.11–33

Baader, F. et al., 2003. The description logic handbook - Theory, Implementation and Applications. *Cambridge University Press*.

Baader, F., Horrocks, I. & Sattler, U., 2005. Description Logics as Ontology Languages for the Semantic Web. *Mechanizing Mathematical Reasoning*, pp.228–248.

Baldwin, W.C. & Sauser, B., 2009. Modeling the Characteristics of System of Systems. *SoSE*, pp.1–6.

Ballard, M., 2013. Why agile development failed for Universal Credit. Available at: http://www.computerweekly.com/news/2240187478/Why-agile-development-failed-for-Universal-Credit.

Balta, D. et al., 2015. E-government Stakeholder Analysis and Management Based on stakeholder interactions and resource dependence. In *48th Hawaii International Conference on System Sciences*.

Barbagallo, A., De Nicola, A. and Missikoff, M. (2010) 'eGovernment Ontologies: Social Participation in Building and Evolution', *2010 43rd Hawaii International Conference on System Sciences*. Ieee, pp. 1–10.

doi: 10.1109/HICSS.2010.174.

Bare, T., 2017. 5 Big Benefits of Workflow Automation for Government. Available at: https://thinksmart.com/5-big-benefits-workflow-automation-government/.

Baum, C.H. & Andrea Di Maio, 2000. Gartner's Four Phases of E-Government Model.

BEA, 2006. The Move Toward Shared Services An Examination of the Business Models.

Behara, G.K., Varre, V.V. & Rao, M., 2009. Service Oriented Architecture for E-Governance. , (October), pp.1–13.

Belhajjame, K. et al., 2013. PROV-DM: The PROV Data Model.

Belhajjame, K. et al., 2015. Using a suite of ontologies for preserving workflow-centric research objects. *Web Semantics: Science, Services and Agents on the World Wide Web*, 32, pp.16–42. Available at: http://dx.doi.org/10.1016/j.websem.2015.01.003.

Benbasat, I. & Zmud, R.W., 2003. The Identify Crisis within the IS Discipline: Defining and Communicating the Discipline's Core Properties. *MIS Quarterly*, 27(2), pp.183–194.

Bergeron, B., 2003. *Essentials of shared services*, John Wiley & Sons, Inc.

Berners-Lee, T., 2006. Linked Data. Available at: https://www.w3.org/DesignIssues/LinkedData.

Bettahar, F., Moulin, C. & A.Barthes, J.-P., 2005. Ontologies supporting e Government Services. In *Artificial intelligence, 2005. epia 2005. portuguese conference*. Covilha: IEEE, pp. 100–105.

Bhattacharya, D., Gulla, U. & Gupta, M.P., 2012. E-service quality model for Indian government portals: citizens' perspective E-service quality model for Indian government portals: citizens' perspective. *Journal of Enterprise Information Management*, 25, pp.246–271. Available at: http://dx.doi.org/10.1108/17410391211224408.

Birkholz, H. et al., 2012. IO: An interconnected asset ontology in support of risk management processes. *Proceedings - 2012 7th International Conference on Availability, Reliability and Security, ARES 2012*, pp.534–541.

Birolini, A., 2014. *Reliability Engineering Theory and Practice* 7th ed., Springer-Verlag Berlin Heidelberg.

Bjarnason, E., Wnuk, K. & Regnell, B., 2011. A Case Study on Benefits and Side-Effects of Agile Practices in Large-Scale Requirements Engineering.

Blackburn, S., 1996. *The Oxford Dictionary of Philosophy*,

Blackwell, C., 2008 'A multi-layered security architecture for modelling complex systems.', in *Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead*, p. 35.

Bloomfield, R. et al., 2010. Stochastic Modelling of the Effects of Interdependencies between Critical Infrastructure. *Critical Information Infrastructures Security Lecture Notes in Computer Science*, pp.201–212.

BMS, 2011. Define Services and explain characteristics of services. Available at: http://www.bms.co.in/define-services-and-explain-characteristics-of-services/.

Boardman, J. & Sauser, B., 2006. System of Systems - the meaning of of. *Smc*, (April), pp.1–6.

Boell, S. & Cezec-Kecmanovic, D., 2011. Are systematic reviews better, less biased and of higher quality? In *ECIS 2011 Proceedings*.

Bolychevsky, I., 2017. Building data infrastructure for personal data. Available at:

https://data.blog.gov.uk/2017/01/19/building-data-infrastructure-for-personal-data/.

Bouet, M. and Israel, M. 2011. 'INSPIRE Ontology Handler : automatically building and managing a knowledge base for Critical Information Infrastructure Protection', pp. 694–697.

Boyce, S. & Pahl, C., 2007. Developing Domain Ontologies for Course Content The Development of Ontologies. , 10, pp.275–288.

Bracken, M., 2015a. Government as a platform: the next phase of digital transformation.

Bracken, M., 2015b. Mapping new ideas for the digital justice system. Available at: https://gds.blog.gov.uk/2015/08/18/mapping-new-ideas-for-the-digital-justice-system-2/.

Brank, J., Grobelnik, M. and Mladenić, D. 2005. 'A survey of ontology evaluation techniques', *Proceedings of the Conference on Data Mining and Data Warehouses*, pp. 166–170. doi: 10.1.1.101.4788.

Brannen, J., 2005. JULIA BRANNEN ESRC National Centre for Research Methods NCRM Methods Review Papers.

Brickley, D. & Guha, R.V., 2014. RDF Schema 1.1.

Brocke, J. vom et al., 2013. International Journal of Accounting Information Systems Living IT infrastructures

Brusa, G., Caliusco, M.L. & Chiotti, O., 2007. Enabling Knowledge Sharing within e-Government Back-Office Through Ontological Engineering. , 2(1), pp.33–48..

Bryman, A., 2001. *Social Research Methods*, Oxford: Oxford University Press.

Bryman, A. & Bell, E., 2015. *Business Research Methods*, Oxford University Press.

Budhraja, A., 2008. Service Oriented Architecture Adoption.

Bureau of Indian Standards, 2009. Iso/Iec 13335-1 : 2004 Information Technology — Security Techniques — Management of Information and Communications Technology Security - PART 1 Concepts and Models for Information and Communications Technology Security Management. *Bureau of Indian Standards*, p.34.

Burégio, V.A. et al., 2006. Specification , Design and Implementation of a Reuse Repository. *Design*, (Compsac), pp.0–3.

Bürger, T., Simperl, E. & Tempich, C.D., 2013. Methodologies for the creation of semantic data. In *Handbook of Metadata, Semantics and Ontologies*. pp. 185–215.

Burgess, J.P., 2007. Social values and material threat: the European Programme for Critical Infrastructure Protection. *International Journal of Critical Infrastructures*, 3(3/4), pp.471–487.

Butler, T., 1998. Towards a hermeneutic method for interpretive research in information systems. *Journal of Information Technology*, 13, pp.285–300.

Byrne, J. & Humble, Á.M., 2007. An Introduction to Mixed Method Research. , pp.1–4.

Cabinet Office, 2004. *e-Government Metadata Standard*,

Cabinet Office, 2008. National Risk Register.

Cabinet Office United Kingdom, 2014. 7 reasons why the UK is a D5 world leader in digital public services. Available at: https://www.gov.uk/government/news/7-reasons-why-the-uk-is-in-the-d5-world-leaders-in-digital-public-services.

Cabinet Office United Kingdom., 2011. Government ICT Strategy. *London:Cabinet Office United Kingdom.*,

(March).

Campion-awwad, O., Hayton, A. & Vuaran, M., 2014. The National Programme for IT in the NHS A Case History. , (February).

CAPEC 2015. 'A Community Knowledge Resource for Building Secure Software'.

CAPEC 2018. 'Common Attack Pattern Enumeration and Classification'. Available at:

https://capec.mitre.org/.

Capgemini, 2006. *Online Availability of Public Services : How Is Europe Progressing ?*,

Capodieci, P. et al., 2010. MICIE: An Alerting Framework for Interdependent Critical Infrastructures. In E. Di Nitto & R. Yahyapour, eds. *Towards a Service-Based Internet: Third European Conference, ServiceWave 2010, Ghent, Belgium, December 13-15, 2010. Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 207–208. Available at: http://dx.doi.org/10.1007/978-3-642-17694-4_26.

Caralli, R.A., 2007. Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process. , (May).

Carney, D., Fisher, D. & Place, P., 2005. Topics in Interoperability : System-of-Systems Evolution. , (March).

CEDAR 2016. *CEDAR User Scenarios*. Available at: https://metadatacenter.org/purpose/scenarios

(Accessed: 15 June 2018).

Chan, F.K.Y. et al., 2010. Modeling Citizen Satisfaction with Mandatory Adoption of an E-Government Technology Journal of the Association for Information Modeling Citizen Satisfaction with Mandatory Adoption of an E-Government Technology. , (March 2014).

Chandana, 2017. Risk register - An important component of overall risk management framework. Available at: https://www.simplilearn.com/risk-management-framework-article.

Chapin, F.S. et al., 2010. Ecosystem stewardship: sustainability strategies for a rapidly changing planet. *Trends in Ecology and Evolution*, 25(4), pp.241–249.

Charalabidis, Y., 2015. Controlled Vocabularies and Metadata Sets for Public Sector Information Management. , (November 2015), pp.25–26.

Chen, Y. N. *et al.* 2006. 'E-Government Strategies in Developed and Developing Countries: An Implementation Framework and Case Study', *Journal of Global Information Management*, 14(1), pp. 23–46

Choudhari, R.D., Banwet, D.K. & Gupta, M.P., 2007. Identifying Risk Factors in for E-governance Projects. , pp.270–277.

Christiansen, J., 2015. Redesigning the culture and functionality of government. Available at: http://designforeurope.eu/news-opinion/redesigning-culture-and-functionality-government.

COBIT, 2012. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*,

Cordall, G. 2012 'Service Level Agreements'.

Corydon, B., Ganesan, V. & Lundqvist, M., 2016. Transforming government through digitization. , (July 2015).

Costa, D. et al., 2016. An Insider Threat Indicator Ontology. , (CMU/SEI-2016-TR-007). Available at: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=454613.

Coyne, R.M., 1995. *Designing Information Technology in the Postmodern Age: From Method to Metaphor*,

Creative Commons, 2011. Beyond Access : Open Government Data & the Right to (Re) use Public Information.

Creative Commons, 2010. Koordinates: NZ open data platform. Available at: http://creativecommons.org.nz/2010/10/koordinates-the-one-place-for-geodata/.

Cregan, A. M. 2008. 'Overview of Semantic Technologies'.

Croope, S. & McNeil, S., 2011. Improving Resilience of Critical Infrastructure Systems Postdisaster. *Transportation Research Record: Journal of the Transportation Research Board*, 2234, pp.3–13. Available at: http://dx.doi.org/10.3141/2234-01.

Crothers, H., 2009. Methods to Create Unique Asset IDs. Available at: https://blogs.esri.com/esri/arcgis/2009/08/03/methods-to-create-unique-asset-ids/.

Crotty, M., 1998. *The Foundations of Social Research: Meaning and Perspectives in the Research Process*, SAGE Publications Inc.

Crown Commercial Service, 2017. Communication Services. Available at: https://ccs-agreements.cabinetoffice.gov.uk/contracts/rm3796.

Crucitti, P., Latora, V. & Marchiori, M., 2004. A topological analysis of the Italian electric power grid. *Physica A: Statistical Mechanics and its Applications*, 338(1-2 SPEC. ISS.), pp.92–97.

CSC, 2011. CSC CATALYST Ontology White Paper.

Curras, E., 2013. Ontologies in Systems Theory. In *Handbook of Metadata, Semantics and Ontologies*. pp. 89–107.

D'Atri, A., Missikoff, O. & De nicola, A., 2008. A Business Ontology for supporting cross border cooperation between european chambers of commerce. , (April).

Daglio, M., D., G. & H., K., 2014. Innovating the Public Sector: from Ideas to Impact. , (November).

Dale Compton, W. et al., 2005. *Building a Better Delivery System: A New Engineering/Health Care Partnership*, National Academies Press US. Available at: http://www.ncbi.nlm.nih.gov/books/NBK22878/.

Damljanovic, D. et al., 2008. A Text-based Query Interface to OWL Ontologies.

Daniel, K., 2015. How to Run an Agile Project in Government. Available at: https://www.digitalgov.gov/2015/01/16/how-to-run-an-agile-project-in-government/.

Datt, S., 2015. Developing conceptual framework in a research paper.

Datt, S. & Datt, S., 2016. Importance of ethical considerations in a research.

David Elkind, 2004. The problem with constructivism. *The Educational Forum*, 68(4).

Davies, J., Studer, R. & Warren, P., 2006. *Semantic Web Technologies: trends and reseacrh in ontology based systems*, West Sussex, England: John Wiley and Sons Limited. Available at: http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1965514&tool=pmcentrez&rendertype=abstract..

Davis, I. & Galbraith, D., 2012. BIO : A vocabulary for biographical information. , pp.1–40.

Davis, K., 2015. Risk Angles-Third Party Risk.

Dawes, S.S., 2008. The evolution and continuing challenges of E-governance. *Public Administration Review*, 68(SUPPL. 1).

DEA, 2013. Risk Management – Guide –.

Dearden, L., 2017. Prisons released 71 inmates in error over the last year in England and Wales as violence surges to new high. *The Independent*. Available at: http://www.independent.co.uk/news/uk/home-news/uk-prison-statistics-71-inmates-released-error-england-wales-service-safety-reoffending-home-office-a7862346.html.

Defra, 2014. Clarifying the application of the definition of waste to re-use and repair Discussion paper Defra November. , (November). Available at: http://resource.co/sites/default/files/Clarifying-the-application-of-the-Definition-of-Waste.pdf.

DeFranzo, S.E., 2011. What's the difference between qualitative and quantitative research?

Dekkers, M. et al., 2011. A common metadata approach to support eGovernment interoperability.

Dekkers, M. et al., 2014. Open Government Data & the PSI Directive. Available at: https://joinup.ec.europa.eu/sites/default/files/d2.1.2_training_module_1.1_open_government_data_and_the_psi_directive_v1.00_en.pdf.

Dekkers, M., 2011. Towards semantic asset management and Core Vocabularies for e-Government Five maturity levels for metadata management Level 1 Level 2 Level 3 Level 4 Open Metadata for Humans. , (September).

DeLaurentis, D., 2007. Role of humans in complexity of a system-of-systems. In *Digital Human Modeling*. Berlin Springer-Verlag;, pp. 363–371.

DeLaurentis, D., 2005. Understanding Transportation as a System-of-Systems Design Problem. In *43rd AIAA Aerospace Sciences Meeting and Exhibit*. Aerospace Sciences Meetings. American Institute of Aeronautics and Astronautics. Available at: http://dx.doi.org/10.2514/6.2005-123.

Deleu, R. & Clendon, J., 2015. Government Enterprise Architecture. , (June), pp.1–44.

Deloitte, 2014. Asset Management : A Risk-Based Approach Energy & Resources Benchmark Survey.

Denkin, N., 1994. *Handbook of qualitative research* L. YS, ed., SAGE Publications Inc.

Department for Transport, 2011. Information Asset Register. Available at: http://webarchive.nationalarchives.gov.uk/20120817151306/http://www.dft.gov.uk/publications/information-asset-register/.

Department for Transport, 2008. Who we share information with and why. Available at: http://webarchive.nationalarchives.gov.uk/20120817154603/http://www.dft.gov.uk/publications/dft-sharing-information/.

Department for Victorian Communities, 2004. Asset Management Policy , Strategy and Plan: Guidelines for Developing an Asset Management Policy ,. , (August).

Department of Health, 2015. 2010 to 2015 government policy: health and social care integration. Available at: https://www.gov.uk/government/publications/2010-to-2015-government-policy-health-and-social-care-integration/2010-to-2015-government-policy-health-and-social-care-integration.

Dersin, P. (Alstom T., 2014. Technical Committee on " Systems of Systems" - WHITE PAPER. *IEEE-Reliability Society*, (1), pp.1–5.

Downe, L., 2015. Better services with patterns and standards. Available at: https://gds.blog.gov.uk/2015/08/06/better-services-with-patterns-and-standards/.

Downe, L., 2016. What we mean by service design. Available at: https://gds.blog.gov.uk/2016/04/18/what-we-mean-by-service-design/.

Dudenhoeffer, D.D. & Manic, M., 2006. CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis. In E. L. F. Perrone, F. P. Wieland, J. Liu, B. G. Lawson, D. M. Nicol, and R. M. Fujimoto, ed. *Proceedings of the 2006 Winter Simulation Conference*. pp. 478–485.

Dudenhoeffer, D.D., Permann, M.R. & Boring, R.L., 2006. Decision consequence in complex environments: Visualizing decision impact. In *Proceeding of Sharing Solutions for Emergencies and Hazardous Environments. American Nuclear Society Joint Topical Meeting: 9th Emergency Preparedness and Response/11th Robotics and Remote Systems for Hazardous Environment*.

Dudley, M. *et al.* 2015. 'Implementing a citizen-centric approach to delivering government services'. Available at: https://www.mckinsey.com/industries/public-sector/our-insights/implementing-a-citizen-centric-approach-to-delivering-government-services.

Dudovskiy, J., 2016. *The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance*,

Dueñas-Osorio, L. et al., 2007. Interdependent Response of Networked Systems. *Journal of Infrastructure Systems*, 13(3), pp.185–194. Available at: http://dx.doi.org/10.1061/(ASCE)1076-0342(2007)13:3(185).

Dueñas-Osorio, L., Craig, J.I. & Goodno, B.J., 2007. Seismic response of critical interdependent networks. *Earthquake Engineering and Structural Dynamics*, 36(2), pp.285–306.

Dueñas-osorio, L.A., 2005. Interdependent Response of Networked Systems to Natural Hazards and Intentional Disruptions Interdependent Response of Networked Systems to Natural Hazards and Intentional Disruptions. , (December).

Dunleavy, P., 2010. *The Future of Joined-up Public Services*,

Dunton, J., 2016. National Audit Office slams Cabinet Office over shared services "failure." Available at: https://www.civilserviceworld.com/articles/news/national-audit-office-slams-cabinet-office-over-shared-services-%E2%80%9Cfailure%E2%80%9D.

Dzhusupova, Z. et al., 2011. Sustaining Electronic Governance Programs in Developing Countries. In *11th European Conference on eGovernment: Sustaining electronic governance programs in developing countries*. Ljubljana: Academic Conferences Limited, p. 9.

Editors, S.I. & Donnellan, B., 2011. IT Artefact & practice theorizing – pragmatic perspectives. , pp.1–2.

Eggers, W. D. and Macmillan, P. 2015. 'Gov2020: A Journey into the Future of Government'.

Elahi, G., Yu, E. & Zannone, N., 2009. A modeling ontology for integrating vulnerabilities into security requirements conceptual foundations. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 5829 LNCS, pp.99–114.

Emis Health, 2014. EMIS to withdraw legacy systems in England following changes to GP computing requirements.

Erl, T., 2006. *Service-Oriented Architecture: Concepts, Technology and Design*,

Ernst and Young, 2014. Centralized operations- The future of operating models for Risk, Control and Compliance functions.

Espinar, M.Á., 2014. Government Data Openness and Re-Use.

European Commission, 2016. *Accelerating the digital transformation of government*,

European Law Blog, 2013. POMFR: Proportionality Analysis and Models of Judicial Review. Available at: https://europeanlawblog.eu/2013/07/16/pomfr-proportionality-analysis-and-models-of-judicial-review/.

European Union, 2017. Tallinn Declaration on eGovernment.

Eusgeld, I., Nan, C. & Dietz, S., 2011. System-of-systems approach for interdependent critical infrastructures. *Reliability Engineering and System Safety*, 96(6), pp.679–686. Available at: http://dx.doi.org/10.1016/j.ress.2010.12.010.

Ezran, M., Morisio, M. & Tully, C., 2002. *Practical Software Reuse*,

Fallon, M., 2015. Working together to help people with court fees. Available at: https://mojdigital.blog.gov.uk/2015/10/23/working-together-to-help-people-with-court-fees/ [Accessed July 24, 2017].

Fang, Z., 2002. E-Government in Digital Era : Concept , Practice, and Development. *International Journal of The Computer, The Internet and Management*, 10(2), pp.1–22.

Farndale, E., Paauwe, J. & Hoeksema, L., 2009. In-sourcing HR : shared service centres in the Netherlands. , 5192(September).

Featherman, M.S. & Pavlou, P.A., 2003. Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human Computer Studies*, 59(4), pp.451–474.

Fensel, D. et al., 2001. On-To-Knowledge in a Nutshell. , pp.1–5.

Fensel, D., 2004. *Ontologies: A Silver Bullet for Knowledge Management and Electronic Commerce*,

Fenz, S. (2010) 'Security Ontology'.

Ferndndez, M., Gmez-p, A. & Juristo, N., 1997. METHONTOLOGY : From Ontological Art Towards Ontological Engineering. , pp.33–40.

Figueiredo, J.A.S., NunesIII, C.A.L. & Fagundes, M.N., 2014. Considering risk theories in relation to a case study in the south of Brazil.

Firescope, 2013. What is an IT Service? Available at: http://www.firescope.com/blog/index.php/service/.

Fischer, C., Winter, R. & Wortmann, F., 2010. Design Theory. , pp.2006–2009.

Fishenden, J., 2015. A (brief) History of UK Government moves towards a Platform-Based Architecture. Available at: https://ntouk.wordpress.com/2015/05/07/a-brief-history-of-uk-government-moves-towards-a-platform-based-architecture/.

Flatworld business, 2011. Web 1.0 vs Web 2.0 vs Web 3.0 vs Web 4.0 vs Web 5.0 – A bird's eye on the evolution and definition. Available at: https://flatworldbusiness.wordpress.com/flat-education/previously/web-1-0-vs-web-2-0-vs-web-3-0-a-bird-eye-on-the-definition/ [Accessed July 19, 2017].

Fonou-dombeu, J. V. and Huisman, M. (2011) 'Semantic-Driven e-Government : Application of Uschold and King Ontology Building Methodology for Semantic Ontology Models Development', 2(4), pp. 1–20.

Forte, V., 2014. Silo thinking at the NHS, despite "reforms." Available at: https://www.ft.com/content/b8aa33c4-02d5-11e4-a68d-00144feab7de?mhq5j=e1.

Fountain, J., 2001. Building the virtual state: Information technology and institutional change. , (June).

Fraser, J. et al., 2003. Knowledge Management Applied to E-government Services : The Use of an Ontology. , pp.116–126.

Friedman, E. (2016) *Evolution of Big Data Storage: How to Support Real-time Analytics at Scale*.

Frontier Economics Ltd, 2012. *Enablers and barriers to integrated care and implications for Monitor*,

Gadamer, H.-G., 1965. Wahrheit und Methode.

Gallo, C. & Giove, M., 2014. *Study on eGovernment and the Reduction of Administrative*,

Garlan, D., Allen, R. & Ockerbloom, J., 1995. Architectural Mismatch: Why Re-use Is So Hard. *IEEE Software*, 12(6), pp.17–26.

Giacomo, G. De & Lenzerini, M., 1996. TBox and ABox reasoning in Expressive Description Logics. In *KR-96*. Los Altos: M. Kaufmann, pp. 316–327.

Gill, P. et al., 2008. Methods of data collection in qualitative research: interviews and focus groups.

Goble, C., 2016. Method Preservation: workflows and models matter. Available at: https://www.bigdata.cam.ac.uk/events/events-archive/2016-events/our-digital-future-2016/programme/method-preservation-workflows-and-models-matter.

Goel, S., Sherry, A. & Sherry, A.M., 2012. Role of Key Stakeholders in Successful E- Governance Programs : Conceptual Framework Role of Key Stakeholders in Successful E-Governance Programs : Conceptual Framework.

Goetz, J.P. & LeCompte, M.D., 1984. *Ethnography and qualitative design in educational research*, Orlando: Academic Press, Inc.

Goldkuhl, G. & Persson, A., 2006. From e-ladder to e-diamond – re--conceptualising models for public e-services.

Gordon, K. & Dion, M., 2008. Protection of "critical infrastructure" and the role of investment policies relating to national security. *OECD (Organisation for Economic Co-operation and Development)*, (May), p.p. 11.

Government Digital Service, 2016. Gov.UK Pay. Available at: https://www.gov.uk/government/publications/govuk-pay/govuk-pay [Accessed July 24, 2017].

Government Digital Service, 2017a. *Government Transformation Strategy*, Available at: https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy.

Government Digital Service, 2017b. Government Transformation Strategy: business transformation. Available at: https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy-business-transformation [Accessed July 24, 2017].

Government Digital Service, 2017c. Government Transformation Strategy: platforms, components and business capabilities. Available at: https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy-platforms-components-and-business-capabilities.

Government Digital Service, 2017d. Government Transformation Strategy: tools, processes and governance. Available at: https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy-tools-processes-and-governance.

Government Digital Service, 2017e. Government Transformation Strategy: vision and scope. Available at: https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy-vision-and-scope [Accessed July 24, 2017].

Graham, S., 2009. Disrupted Cities : When Infrastructure Fails.

Graves, S., 2013. Reducing Our Debt by Reducing Government Duplication. Available at: https://www.cnbc.com/id/100568845.

Greenhalgh, T. & Taylor, R., 1997. Education and debate How to read a paper : Papers that go beyond numbers (qualitative research) What is qualitative research ? Evaluating papers that describe qualitative research. , 743, pp.740–743.

Grönlund, Å. & Horan, T.A., 2005. Introducing e-Gov : History , Definitions , and Issues. , 15(June).

Gruber, T. R. (1993) 'Toward Principles for the Design of Ontologies Used for Knowledge Sharing', pp. 907–928.

Gruninger, M. & Fox, M.S., 1995. Methodology for the Design and Evaluation of Ontologies 1 Introduction 2 Motivating Scenarios. , pp.1–10.

Gruninger, M., and Fox, M.S., 1995. Methodology for the Design and Evaluation of Ontologies. *Workshop on Basic Ontological Issues in Knowledge Sharing, IJCAI-95,*.

Guba, E.G. & Lincoln, Y.S., 1994. Competing Paradigms in Qualitative Research. In *Handbook of Qualitative Research, Thousand Oak*. SAGE Publications Inc.

Gugliotta A, Cabral Liliana and Domingue John (2005) 'Knowledge modelling for integrating semantic web ser- vices in e-government applications Conference Item'.

Gupta, M.P. & Jana, D., 2003. E-government evaluation: A framework and case study. *Government Information Quarterly*, 20(4), pp.365–387.

Gupta, M.P., Kumar, P. & Bhattacharya, J., 2003. *Government Online*, Tata McGraw-Hill Education, 2003.

Gyawali, B., 2011. *Answering factoid questions via ontologies: A natural language generation approach*.

Haan, N. 2015. *Why We Need Government to Evolve as Fast as Technology*, *Singularity Hub*. Available at: https://singularityhub.com/2015/12/03/why-we-need-government-to-evolve-as-fast-as-technology/#sm.00000321qt1dd4cz4q72vnc51n3z7.

Haberfield, T. and Franklin, K. (2017) 'Mapping the border as users see it'.

Habil D. P. Zukauskas & A. Kasteckiene, 2002. The Role of E-Government in the Development of the new economy in Lithuania.

Hall, K., 2016. Buck up, UK.gov. You need to get a grip on failing shared services centres - PAC. Available at: https://www.theregister.co.uk/2016/10/19/cabinet_office_needs_to_get_a_grip_of_its_shared_services/.

Hall, P. 2016. *How the Government can make a success of Making Tax Digital*. Available at: https://www.conservativehome.com/platform/2016/11/phil-hall-how-the-government-can-make-a-success-of-making-tax-digital.html.

Halligan, J. & Moore, T., 2004. E-government in Australia: The challenges of moving to integrated services.

Han, J. and Chen, P. (2002) 'Architecture support for system-of-systems evolution', *... and Deployment of Cooperative Information Systems*, pp. 332–346. Available at: http://link.springer.com/chapter/10.1007/3-540-45785-2_26.

Harbott, A., 2016. How we're transforming justice: Digital Justice speech at Sprint 16. Available at: https://mojdigital.blog.gov.uk/2016/02/26/how-were-transforming-justice-digital-justice-speech-at-sprint-16/.

Hardy, K. 2010. 'Managing Risk in Government: An Introduction to Enterprise Risk Management', *Financial Management Series*, 2(10), pp. 1–53. Available at: https://www.rims.org/resources/ERM/Documents/Risk in Government.pdf.

Harries, E., Wharton, R. and Abercrombie, R. 2015. 'Systems change: A guide to what it is and how to do it', (June), pp. 1–11.

Hasan, M., 2015. The challenges of e-Government in Palestine.

Havelock, K., 2017a. How we're connecting new services with legacy systems. Available at: https://governmenttechnology.blog.gov.uk/2017/03/31/how-were-connecting-new-services-with-legacy-

systems/ [Accessed May 17, 2017].

Havelock, K., 2017b. How we're connecting new services with legacy systems. Available at: https://governmenttechnology.blog.gov.uk/2017/03/31/how-were-connecting-new-services-with-legacy-systems/.

Hayes, W. et al., 2016. Scaling Agile Methods for Department of Defense Programs. , (December).

Haynes, D., 2004. *Metadata for Information Management and Retrieval*, Facet Publishing, London.

Hearst, M. *et al.* 2002. 'Finding the Flow in Web Site Search 1 The Search Task Continuum', pp. 1–6.

Heath, N., 2013. How even agile development couldn't keep this mega-project on track. Available at: http://www.zdnet.com/article/how-even-agile-development-couldnt-keep-this-mega-project-on-track/.

Heeks, R., 2006. *Implementing and Managing EGovernment: An International Text*, SAGE Publications Inc.

Heeks, R. & Bailur, S., 2007. Analyzing e-government research: Perspectives, philosophies, theories, methods, and practice. *Government Information Quarterly*, 24(2), pp.243–265. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0740624X06000943 [Accessed October 2, 2015].

Hernon, P. et al., 2002. *United States government information: Policies and sources*, Libraries Unlimited.

Herzog, A., Shahmehri, N. and Duma, C. (2007) 'An Ontology of Information Security', *International Journal of Information Security and Privacy*, 1(4), p. 23.

Hevner, A.R. et al., 2004. DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH. , 28(1), pp.75–105.

Hickie, I., 2017. Mental health funding "locked down in dysfunctional hospital system." Available at: https://www.theguardian.com/society/2017/feb/02/mental-health-funding-locked-down-in-dysfunctional-hospital-system-ian-hickie.

Hill, R., 2016. Universal Credit: Poor planning and lack of "agile" expertise major factors in disastrous start, says report. Available at: https://www.publictechnology.net/articles/news/universal-credit-poor-planning-and-lack-%E2%80%98agile%E2%80%99-expertise-major-factors-disastrous.

Hiller, J.S. & Bélanger, F., 2001. Privacy Strategies for Electronic Government. *Center for Global Electronic Commerce*, p.40. Available at: http://www.businessofgovernment.org/sites/default/files/PrivacyStrategies.pdf.

Hinkelmann, K., Thönssen, B. & Wolff, D., 2010. *Theory and Applications of Ontology: Computer Applications* R. Poli, M. Healy, & A. Kameas, eds., Dordrecht: Springer Netherlands. Available at: http://link.springer.com/10.1007/978-90-481-8847-5 [Accessed November 5, 2015].

Hitzler, P. & Parsia, B., 2009. OWL 2 Web Ontology Language Primer. , (October), pp.1–123.

HM Revenue and Customs, 2014. How to comply with EU Payments Regulation. Available at: https://www.gov.uk/guidance/how-to-comply-with-eu-payments-regulation.

HM Treasury, 2004. *The Orange Book Management of Risk - Principles and Concepts*,

Holgeid, K. & Thompson, M., 2013. A Reflection on Why Large Public Projects Fail. , (May).

Holliday, B., 2016. Fixing the broken windows and making design matter. Available at: http://www.hollidazed.co.uk/2016/02/11/broken-windows/.

Holmes, B. 2011. 'Citizens ' engagement in policymaking and the design of public services', (1).

Holmström, J.., Ketokivi, M. & Hameri, A.., 2009. Bridging Practice and Theory: A Design Science Approach.

Decision Science, 40(1), pp.65–87.

Homburg, V., Bekkers, V. & Rotterdam, N., 2002. The Back-Office of E-Government (Managing Information Domains as Political Economies) Center for Public Management The Dutch Setting : Networks of Governmental Organizations and The Political Economy of Information. , 00(c), pp.1–9.

Horridge, M. et al., 2011. A Practical Guide To Building OWL Ontologies Using Prot´eg´e 4 and CO-ODE Tools Edition 1.3.

Horridge, M. et al., 2007. Matthew Horridge, Simon Jupp, Georgina Moulton, Alan Rector, Robert Stevens, Chris Wroe.

Horridge, M. & Bechhofer, S., 2009. The OWL API: A Java API for OWL ontologies. *Semantic Web*, 2(1), pp.11–21.

Hough, J. 2014. 'Changing systems for people with multiple needs : Learning from the literature', 44(1055254).

House of Commons, 2013. House of Commons Committee of Public Accounts Integration across government and Whole – Place Community Budgets. , (September).

IBM News Room, 2016. IBM Security To Expand Incident Response Capabilities With Plans To Acquire Resilient Systems.

IBM UK, 2006. Shared Services.

IBM United States, 2014. Software withdrawal and support discontinuance : IBM System Storage DR550 File System Gateway Software 5639-DR1 and 1 year Software Maintenance (SWMA) PIDs - No replacements available. , pp.1–2.

ICO, 2016. The Guide to Freedom of Information. , pp.1–63.

InfoWorld, 2004. integrating services with legacy systems in government. *26*, p.40.

Institute of Medicine (US) Committee on Quality of Health Care in America. (2001) 'Crossing the Quality Chasm: A New Health System for the 21st Century', in *Formulating New Rules to Redesign and Improve Care.*

ISA^2, 2017. EIF and ISA^2 highlighted in new Ministerial Declaration on e-Government. Available at: https://ec.europa.eu/isa2/news/european-interoperability-framework-and-isa%C2%B2-highlighted-new-ministerial-declaration-e_en.

ISEB, 2010. Reference Model for ISEB Certificates in Enterprise and Solution Architecture. , (June).

ISO, 2008. ISO/IEC 12207:2008 Systems and software engineering - Software life cycle processes.

ISO 31000, 2009. Risk Management. Available at: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso_31000_for_smes.pdf.

ISO 55000, 2014. What is Asset Management? Available at: https://theiam.org/What-is-Asset-Management.

ISO/IEC 27002, 2005. Information technology -- Security techniques – Code of practice for information security management.

ISO/IEC 27005, 2011. Information technology -- Security techniques -- Information security risk management. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en.

ITIL, 2011. ITIL 2011 glossary and abbreviations.

Jabareen, Y., 2009. Building a Conceptual Framework : Philosophy , Definitions , and Procedure. , pp.49–62.

Jacob, E., 1987. Qualitative Research Traditions: A Review. *Review of Educational Research*, 57(1), pp.1–50.

Jacobs, D. & Harris, A., 2015. Introduction to ITIL : A Framework for IT Service Management.

Jaeger, P.T., 2003. The endless wire: E-government as global phenomenon. *Government Information Quarterly*, 20(4), pp.323–331.

Janowski, T., 2015. Digital government evolution : From transformation to contextualization. *Government Information Quarterly*, 32(3), pp.221–236. Available at: http://dx.doi.org/10.1016/j.giq.2015.07.001.

Janssen, M. et al., 2013. Government Architecture : Concepts , Use and Impact. In *12th International Conference on Electronic Government (EGOV)*. Koblenz, Germany: Springer, pp. 135–147.

Janssen, M. & Joha, A., 2006. Motives for establishing shared service centers in public administrations. , 26, pp.102–115.

Janssen, M. & Wagenaar, R., 2004. Developing Generic Shared Services for e- Government. *Electronic Journal of E-Government*, 2(1), pp.31–38.

Jeong, B., Cho, H. & Lee, C., 2009. On the functional quality of service (FQoS) to discover and compose interoperable web services. *Expert Systems with Applications*, 36(3), pp.5411–5418.

Johansson, J., 2010. *Risk and Vulnerability Analysis of Interdependent Technical Infrastructures Addressing Socio-Technical Systems*.

Johansson, J., Hassel, H. & Cedergren, A., 2011. Vulnerability analysis of interdependent critical infrastructures: Case study of the Swedish railway system. *International Journal of Critical Infrastructures*, 7(4), pp.289–316.

Johnson, E., 2015. Lessons Learned from the Failure of Agile Development. Available at: https://intland.com/blog/agile/failure-of-agile/.

Jupp, V., 2006. Critical Research.

Kaiser, A., 2015. ITIL Foundation : Types of Service Providers. Available at: http://abhinavpmp.com/2015/07/08/itil-foundation-types-of-service-providers/.

Kaplan, R.S. & Mikes, A., 2012. Managing Risks: A New Framework. Available at: https://hbr.org/2012/06/managing-risks-a-new-framework.

Karagiannis, D., 2009. Modelling Semantic Workflows for E-Government Applications.

Kaufmann, E. & Bernstein, A., 2007. How Useful Are Natural Language Interfaces to the Semantic Web for Casual End-Users ? , pp.281–294.

Keith, T., 2017. Why Eliminating Government Agencies Is A Lot Easier Said Than Done. Available at: http://www.npr.org/2017/03/17/520483474/why-eliminating-government-agencies-is-a-lot-easier-said-than-done.

Kelly, S. 2014 'The cost of cascading failure'.

Kelly, S. *et al.*, 2016. 'Exploring Vulnerability and Interdependency of UK Infrastructure Using Key-Linkages Analysis', pp. 865–892. doi: 10.1007/s11067-015-9302-x.

Keng Siau & Yuan Long, 2005. Synthesizing e-government stage models - a meta-synthesis based on meta-ethnography approach. *Industrial Management {&} Data Systems*, 105(4), pp.443–458. Available at: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=17530894&site=ehost-live.

Kernaghan, K., 2012. INTEGRATED SERVICES. *Encyclopedic Dictionary of Public Administration*.

King, J.L. & Lyytinen, K., 2004. Reach and Grasp. *MIS Quarterly*, 28(4), pp.539–551.

Kjølle, G.H., Utne, I.B. & Gjerde, O., 2012. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. *Reliability Engineering and System Safety*, 105, pp.80–89. Available at: http://dx.doi.org/10.1016/j.ress.2012.02.006.

Klaver, M.H.A. et al., 2015. Critical Infrastructure Assessment by Emergency Management.

Klein, H.K. & Myers, M.., 1999. A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly*, 23(1), pp.67–93.

Klischewski, R., 2003. Semantic Web for e-Government.

KMD, 2016. *Unlocking the eGovernment in Europe*,

Kollarits, S. et al., 2009. RISK ONTOLOGY MONITOR – an ontological basis for risk management together with Document history. , pp.1–76.

Korte, G., 2014. Government often has 10 agencies doing one job. Available at: https://www.usatoday.com/story/news/politics/2014/04/08/billions-spent-on-duplicate-federal-programs/7435221/.

Korte, G., 2013. Redundant federal programs waste billions. Available at: https://www.usatoday.com/story/news/politics/2013/04/09/wasteful-government-spending/2063511/.

Kotov, V., 1997. Systems of Systems as Communicating Structures. , HPL-97-124, pp.1–15.

Kramer, J. & Magee, J., 1985. Dynamic Configuration for Distributed Systems. *IEEE Transactions on Software Engineering*, SE-11(4), pp.424–436.

Krell, K., Matook, S. & Rohde, F., 2008. Understanding Information System Change: the Relation Between Reasons, Goals, and Types. *12th Pacific Asia Conference on Information Systems*, pp.1202–1213. Available at: <Go to ISI>://WOS:000262877100101.

Krivin, D. et al., 2013. Managing third-party risk in a changing regulatory environment. , (46).

Kucera, J. & Chlapek, D., 2014. Benefits and Risks of Open Government Data. *Journal of Systems Integration*, 5(1).

Kuhn, T.S., 1962. *The Structure of Scientific Revolutions*,

Kunstelj, M. & Leben, A., 2002. DELIVERING BETTER QUALITY PUBLIC SERVICES THROUGH LIFE-EVENT PORTALS 2 LIFE-EVENT APPROACH. , pp.1–15.

Kwon, Y., Kim, E. & Lee, N., 2015. Key Factors on Software Reuse of e-Government Common Framework.

Lakatos, I., 1978. *The methodologyof scientific research programmes* J. Worrall & G. Currie, eds., Cambridge University Press.

Lamb, J., 2008. Legacy systems continue to have a place in the enterprise. Available at: http://www.computerweekly.com/feature/Legacy-systems-continue-to-have-a-place-in-the-enterprise.

Lamharhar, H., Chiadmi, D. and Benhlima, L. (2015) 'Ontology-based Knowledge Representation for e-Government Domain', in *Proceedings of the 17th International Conference on Information Integration and Web-based Applications & Services*. New York, NY, USA: ACM (iiWAS '15), p. 51:1--51:10. doi: 10.1145/2837185.2837203.

Lampathaki, F., Kroustalias, N. & Psarras, J., 2010. Implementing Interoperability Infrastructures : Issues and Challenges from the Citizens ' Base Registry in Greece. , pp.1–10.

Landwehr, C.E. et al., 1994. A taxonomy of computer program security flaws. *ACM Computing Surveys*, 26(3), pp.211–254.

Lankhorst, M.M., 2005. Enterprise architecture modelling — the issue of integration. , 18(2004), pp.205–216.

Laryea, S., Badu, E. & Dontwi, I.K., 2007. The price of risk in construction projects : Contingency Approximation Model (CAM). , pp.1–13.

Laugé, A., Sarriegi, J.M. & Hernantes, J., 2013. Disaster Impact Assessment: A Holistic Framework. *Proceedings of the 10th International ISCRAM Conference – Baden-Baden, Germany, May 2013*, (May), pp.730–734. Available at: http://www.iscramlive.org/ISCRAM2013/files/225.pdf\nhttp://www.iscramlive.org/ISCRAM2013/files/225.pdf TS - RIS.

Lauge´, A., Hernantes, J. & Sarriegi, J.M., 2015. Critical infrastructure dependencies: A holistic, dynamic and quantitative approach. *International Journal of Critical Infrastructure Protection*, 8, pp.16–23. Available at: http://dx.doi.org/10.1016/j.ijcip.2014.12.004.

Layne, K. and Lee, J.,2001. 'Developing fully functional E-government: A four stage model', *Government Information Quarterly*, 18(2), pp. 122–136. doi: 10.1016/S0740-624X(01)00066-1.

Lee, E.E., Mitchell, J.E. & Wallace, W.A., 2007. Restoration of Services in Interdependent Infrastructure Systems : A Network Flows Approach. , 37(6), pp.1303–1317.

Lee, E.E., Mitchell, J.E. & Wallace, W.A., 2007. Restoration of services in interdependent infrastructure systems: a network flows approach. *IEEE Transactions on systems, Man, and Cybernetics—part C: Application and Reviews,*, 37(6), pp.1303–1317.

Lee, J., 2006. 'The Roles of Scenario Use in Ontology Development', *Wiley InterScience*, 13(4), pp. 270–284. doi: 10.1002/kpm.

Lehman, M.., 1978. Laws of Program Evolution —Rules and Tools for Programming Management April. In *Infotech State of the Art Conference,*. pp. 1–25.

Lehman, M.., 1974. Programs, Cities, Students, Limits to Growth? *Inaugural Lecture, in Imperial College of Science and Technology Inaugural Lecture Series*, pp.211–229.

Lexis Nexis, 2010. Stemming the Tidal Wave : Data Integration Platform Helps Government Agencies Meet National Security Challenges Manage large-scale disparate data challenges . , (February).

Li, S.H. & Wang, K.C., 2009. Applications of ontology in management of information asset. *IIH-MSP 2009 - 2009 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp.230–233.

Lillbacka, R.G. V, 2013. Realism , Constructivism , and Intelligence Analysis Realism , Constructivism , and. , 0607(November).

Lim, S.-K. & Ko, I.-Y., 2009. Collaborative Ontology Construction Using Template-Based Wiki for Semantic Web Applications. *2009 International Conference on Computer Engineering and Technology*, pp.171–175. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4769581 [Accessed October 6, 2015].

Lincoln, Y.S. & Guba, E.G., 1989. *Fourth Generation Evaluation*, SAGE Publications Inc.

Lindgren, I., 2013. *Public e-Service Stakeholders A study on who matters for public e-service development and implementation*,

Lindgren, I. & Jansson, G., 2014. Electronic services in the public sector : A conceptual framework Electronic services in the public sector : A conceptual framework. , (April 2013).

Lipsky, M., 1980. *Street-level Bureaucracy: Dilemmas of the Individual in Public Services.* Russell Sage Foundation.

Lipson, H., 2006. Evolutionary Systems Design : Recognizing Changes in Security and Survivability Risks. , (September).

Little, R.G. et al., 2012. Managing the Risk of Aging Infrastructure. , (November), pp.1–37.

Lock, R., 2012. Developing a methodology to support the evolution of System of Systems using risk analysis. *Systems Engineering*, 15(1), pp.62–73.

Lock, R., 2011. Modelling and analysing standard use within system of systems. *Proceedings - 2011 16th IEEE International Conference on Engineering of Complex Computer Systems, ICECCS 2011*, pp.149–156.

Lock, R. & Sommerville, I., 2010. Modelling and analysis of socio-technical system of systems. In *15th IEEE International Conference on Engineering of Complex Computer Systems*. IEEE.

London, S.,1996. 'Understanding Change: How It Happens and How to Make It Happen'.

MacDermott, ??ine et al., 2014. Simulating critical infrastructure cascading failure. *Proceedings - UKSim-AMSS 16th International Conference on Computer Modelling and Simulation, UKSim 2014*, (MARCH), pp.324–329.

Macintosh, E.A. et al., 2003. A Governmental Knowledge-based Platform for Public Sector Online Services Deliverable D71 : A Framework for e-Government Services.

Mack, N. et al., 2005. *Qualitative Research Methods: A DATA COLLECTOR'S FIELD GUIDE*,

Magoutas, B., Halaris, C. & Mentzas, G., 2007. An Ontology for the Multi-perspective Evaluation of Quality in E-Government Services. *Electronic Government: 6th International Conference, (EGOV 2007)*, 4656/2007, pp.318–329. Available at: http://www.springerlink.com/content/p78w21624g1k7213/?p=426788d0198743f4b3974a62452d4c56&pi=26.

Mahmoud, Q. H., 2004. 'Developing Web Applications with JavaServer Faces'. Available at:

https://www.oracle.com/technetwork/articles/java/javaserverfaces-135231.html.

Maier, M.W., 2006. Architecting Principles for Systems-of-Systems. Available at: https://archive.is/Rcc6e#selection-6.3-289.13 [Accessed June 28, 2016].

Maier, M.W., 1998. Architecting Principles for Systems-of-Systems. *Systems Engineering*, 1(4), pp.267–284.

Majchrzak, A., Cooper, L.P. & Neece, O.E., 2004. Knowledge Reuse for Innovation. *Management Science*, 50(2), pp.174–188.

Manola, F. & Miller, E., 2004. RDF Primer. Available at: https://www.w3.org/TR/rdf-primer/.

Manuel E. Prieto Méndez, V.H.M.D. & Castro, C.L.V., 2013. METADATA AND ONTOLOGIES IN E-LEARNING World. In *Handbook of Metadata, Semantics and Ontologies*.

March, S.. & Smith, G., 1995. Design and Natural Science Research on Information Technology. *Decision Support Systems*, 15(4), pp.251–266.

Margetts, H., 2017. *In a digital society, governments should innovate with the best of them*, *World Economic Forum*.

Markus, M.L. & Robey, D., 1988. Information technology and organizational change: Causal structure in theory and research.

Maynard, D.,2006. ‘Metrics for Evaluation of Ontology-based Information Extraction’.

McBride, B., 2004. RDF Primer: W3C Recommendation. Available at: http://www.w3.org/TR/2004/REC-rdf-primer-20040210/.

McCartney, M., 2016. Breaking down the silo walls. Available at: http://www.bmj.com/content/354/bmj.i5199.

McCoy, K.F., 2012. Natural language generation and assistive technologies. , p.1. Available at: http://dl.acm.org/citation.cfm?id=2392712.2392714.

McGregor, M., 2012. Who Is Using Open Government Data? Available at: http://creativecommons.org.nz/2012/10/who-is-using-open-government-data/.

McGuinness, D.L. & Harmelen, F. van, 2004. OWL Web Ontology Language Overview: W3C Recommendation. Available at: http://www.w3.org/TR/owl-features/.

McKay, J. & Marshall, P., 2005. A Review of Design Science in Information Systems. In *Proceedings of the 16th Australasian Conference on Information Systems*. Sydney, Australia.

Menachemi, N. & Collum, T.H., 2011. Benefits and drawbacks of electronic health record systems. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3270933/.

Menascé, D.A., Casalicchio, E. & Dubey, V., 2010. On optimal service selection in Service Oriented Architectures. *Performance Evaluation*, 67(8), pp.659–675. Available at: http://dx.doi.org/10.1016/j.peva.2009.07.001.

Menzel, C.P. & Mayer, R.J., 1992. IDEF5 Ontology Description Capture Method : Concepts and Formal Foundations

Merwe, B. van der, 2016. Redesigning government innovation. Available at: https://www.fjordnet.com/conversations/redesigning-government-innovation/.

MetricStream, 2017. Third-Party Due Diligence. Available at: http://www.metricstream.com/solution_briefs/third-party-due-diligence.htm.

Meulen, R. van der, 2016. When Less Becomes More: The Journey to Digital Government. Available at: http://www.gartner.com/smarterwithgartner/when-less-becomes-more-the-journey-to-digital-government/ [Accessed July 19, 2017].

Michael Stewart, 2014. Who’s in charge? Available at: https://www.networks.nhs.uk/discussion/a-lifeboat-for-nhs-managers/871115890.

Mike Bracken, 2015. Same, but different: a common international approach to digital government. Available at: https://gds.blog.gov.uk/2015/07/29/same-but-different-a-common-international-approach-to-digital-government/ [Accessed July 22, 2017].

Mikelakis, M. & Papatheodorou, C., 2012. An ontology-based model for preservation workflows.

Miles, M.B. & Huberman, M.A., 1994. *Quantitative Data Analysis: An expanded sourcebook*, Beverly Hills: SAGE Publications Inc.

Miles, T., 2011. Applying shared services to public sector property and facilities asset management. In *IET and IAM Asset Management Conference*. pp. 1–5.

Miller, P.D., 2014. In Praise of Simple Government. Available at: http://thefederalist.com/2014/01/29/in-praise-of-simple-government/.

Mingers, J., 2003. A Classification of the Philosophical Assumptions of Management Science Methods. *The Journal of the Operational Research Society*, 54(6).

Ministerial Declaration on eGovernment, 2009. Ministerial Declaration on eGovernment. , (November 2009).

Miskon, S. et al., 2010. Understanding shared services: An exploration of the IS literature. *nternational Journal of E-Services & Mobile Applications*, 2(4), pp.373–384.

Mizoguchi, R., 2004. Ontology Engineering Environments. , pp.1–20.

Mockus, A. and Votta, L., 2000. 'Identifying reasons for software changes using historic databases', *Proceedings International Conference on Software Maintenance ICSM-94*, pp. 120–130. doi: 10.1109/ICSM.2000.883028.

Money, L., 2016. Making it easier for staff to process help with court fees applications. Available at: https://mojdigital.blog.gov.uk/2016/01/05/making-it-easier-for-staff-to-process-help-with-court-fees-applications/.

Monroe, M.A., 2015. Government Services Through a Life Events Approach. Available at: https://www.digitalgov.gov/2015/05/15/government-services-through-a-life-events-approach/.

Moon, M.J., 2002. The Evolution of E-Government among Municipalities: Rhetoric or Reality? *Public Administration Review*, 62(4), pp.424–433. Available at: http://onlinelibrary.wiley.com/doi/10.1111/0033-3352.00196/full\npapers3://publication/uuid/5631297A-0B6D-4F58-A835-2E56BB79C9E1.

Moon, M.J., Lee, J. & Roh, C., 2014. *Administration & Society*,

Mueller, T., Harvey, D. & Johnson, S., 2015. Making Agile Work in Government. , (May).

Mundy, D. and Musa, B.,2010. 'Towards a Framework for eGovernment Development in Nigeria Independent Researcher , UK', 8(2), pp. 148–161.

Munir, K. and Anjum, M. S., 2018. 'Applied Computing and Informatics The use of ontologies for effective knowledge modelling and information retrieval', *Applied Computing and Informatics*. King Saud University, 14(2), pp. 116–126. doi: 10.1016/j.aci.2017.07.003.

Mutula, S.M., 2008. Comparison of sub-Saharan Africa's e-government status with developed and transitional nations. *Information Management & Computer Security*, 16(3), pp.235–250.

Myers, M.., 2009. *Qualitative research in business and management*, London: SAGE Publications Inc.

Napier, J.R., 2013. Workflow Management Improves Public Service. Available at: http://www.govtech.com/e-government/Workflow-Management-Improves-Public-Service.html.

National Archives, 2014. UK implementation of Directive 2013/37/EU on the reuse of public sector information. Available at: https://www.gov.uk/government/consultations/uk-implementation-of-directive-201337eu-on-the-reuse-of-public-sector-information.

National Audit Office, 2013a. A snapshot of the use of Agile delivery in central government.

National Audit Office, 2017a. Digital transformation in government. , (March).

National Audit Office, 2017b. Health and social care integration. , (February).

National Audit Office, 2011. Managing risks in government.

National Audit Office, 2013b. Managing the risks of legacy ICT to public service delivery. , (September).

National Audit Office, 2012. Reorganising central government bodies. , (January).

National Audit Office, 2000. Supporting innovation : Managing risk in government departments Supporting innovation : Managing risk in government departments. , (August).

National Cyber Security Centre, CESG Information Assurance Standard 1 & 2.

Neuhaus, F. *et al.*, 2013. 'Ontology Summit 2013 Communiqué : Towards Ontology Evaluation across the Life Cycle 1 . Executive Summary Problem 2 . Purpose of this Document', pp. 1–14.

Ngulube, P., 2007. The Nature and Accessibility of E-Government in Sub Saharan Africa. *International Review of Information Ethics*, 7, pp.1–13. Available at: http://fiz1.fh-potsdam.de/volltext/ijie/08092.pdf.

NHS Alliance, 2008. Integrated Care Organisations : the importance of integrated information systems.

NHS Monitor, 2015. Delivering better integrated care. Available at: https://www.gov.uk/guidance/enabling-integrated-care-in-the-nhs.

Niemann, B. et al., 2005. Introducing Semantic Technologies and the Vision of the Semantic Web Introducing Semantic Technologies and the Vision of the Semantic Web. *Semantic Interoperability Community of Practice (SICoP)*.

Nieuwenhuijs, A., Luiijf, E. & Klaver, M., 2008. Modeling Dependencies in Critical Infrastructures. In P. Mauricio & S. Shenoi, eds. *Critical Infrastructure Protection II*. Boston: Springer, pp. 205–214.

Nilsson, M. & Baker, T., 2008. Notes on DCMI specifications for expressing Dublin Core metadata in RDF.

NIST, 2012. Guide for conducting risk assessments. , (September), p.95. Available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf\nhttp://csrc.nist.gov/publications/PubsSPs.html\nhttp://dx.doi.org/10.6028/NIST.SP.800-30r1.

NIST 1995. *An Introduction to Computer Security: The NIST Handbook*.

Norris, C., 2005. *Epistemology: Key Concepts in Philosophy*,

NOU, 2006. *Official Norwegian Report:When security is the most important*, Oslo.

NWSI 80-202, 2014. System Decommissioning Process.

O'Reilly, T., 2010. *Government as a platform*,

OECD, 2008. Future of e-government AGENDA 2020. *OECD E-Leaders Conference 2008*. Available at: www.oecd.org/dataoecd/41/40/43340370.pdf.

OECD, 2003. *OECD e-Government Studies The e-Government Imperative*, OECD Publishing. Available at: https://books.google.co.uk/books?id=E7X73oFkwV0C.

OECD, 2009. *Overcoming Barriers to Administrative Simplification Strategies*,

OECD, 2014. *Risk Management and Corporate Governance*,

Ojo, A. & Janowski, T., 2005. Ontology, Semantic Web and Electronic Government.

OMG, 2005. *Reusable asset specification*,

Orlikowski, W.J. & Baroudi, J.J., 1991. Studying Information Technology in Organizations: Research Approaches and Assumptions.

Orlikowski, W.J. & Iacono, C.S., 2001. Research Commentary: Desperately Seeking the "IT" in IT Research—A Call to Theorizing the IT Artifact. *Information Systems Research*, 12(2), pp.121–134. Available at: https://pubsonline.informs.org/doi/abs/10.1287/isre.12.2.121.9700.

Ostasius, E., Petraviciute, Z. & Kulvietis, G., 2010. CONSTRUCTING A GENERIC E-SERVICE MODEL IN PUBLIC SECTOR. In *16th International Conference on Information and Software Technologies IT-2010*.

Kaunas, Lithuania, pp. 33–40.

Osterweil, L., Millett, L.I. & Winston, J.D., 2007. *Social Security Administration Electronic Service Provision: A Strategic Assessment*,

Ostroff, F., 2006. Change Management in Government. Available at: https://hbr.org/2006/05/change-management-in-government.

Ouchetto, H., Ouchetto, O. & Roudiès, O., 2012. Ontology-oriented e-gov services retrieval. *IJCSI International Journal of Computer Science*, 9(2), pp.99–107.

Ouyang, M. et al., 2009. A methodological approach to analyze vulnerability of interdependent infrastructures. *Simulation Modelling Practice and Theory*, 17(5), pp.817–828. Available at: http://dx.doi.org/10.1016/j.simpat.2009.02.001.

Ouyang, M., 2014. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering and System Safety*, 121, pp.43–60. Available at: http://dx.doi.org/10.1016/j.ress.2013.06.040.

OWL 2004. *OWL Web Ontology Language Overview*. Available at: Web Ontology Language (OWL),.

Palmaers, T., 2013. Implementing a vulnerability management process. *Information Security*, p.23.

Pansiri, J., 2006. Pragmatism : A methodological approach to researching strategic alliances in tourism Pragmatism : A Methodological Approach to Researching Strategic Alliances in Tourism. , 0548(November).

Papazoglou, M.P. et al., 2008. Service-oriented computing: a research roadmap. , 17(2), pp.223–255.

Parrado, S., 2002. ICT related skills for e-government. In *Seminar on reform of public administrations, OECD*. Paris.

PASC, 2011. Government and IT — " a recipe for rip-offs ": time for a new approach. , (July).

PASC, 2014a. Oral evidence: Accountability of quangos and public bodies. Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/public-administration-committee/accountability-of-quangos-and-public-bodies/oral/11477.html.

PASC, 2014b. Who ' s accountable ? Relationships between Government and arm ' s-length bodies. , (November).

Patel, S., 2015. The research paradigm – methodology, epistemology and ontology – explained in simple language. Available at: http://salmapatel.co.uk/academia/the-research-paradigm-methodology-epistemology-and-ontology-explained-in-simple-language.

Patel-Schneider, P.F., 2004. Tutorial on the W3C OWL Web Ontology Language. In *ENC 2004*. Available at: http://ect.bell-labs.com/who/pfps/talks/owl-tutorial/.

Pattison, S., 2006. Eliminating Silos in Government. *Insight*.

Paunović, L. et al., 2012. The impact of applying the concept of the Semantic Web in e-government.

PCCIP, 1997. *Critical foundations: protecting America's infrastructures: the report of the President's commission on critical infrastructure protection*, Washington, DC: U.S. Government Printing Office.

PCI-DSS, 2004. Payment Card Industry Security Standard Council, "PCI Data Security Standard."

Peerenboom, J.P. et al., 2002. Studying the chain reaction. *Electric Perspectives*, 27(1), pp.22–35.

Peffers, K. et al., 2008. A design science research methodology for information systems research. *Manage Info*

Syst, 24(3), pp.45–77.

Peffers, K. et al., 2007. A Design Science Research Methodology for Information Systems Research. , 24(3), pp.45–78.

Pentti, R., 2007. Finding Information in Texts.

Persson, A. & Goldkuhl, G., 2005. Stage-models for public e-services-investigating conceptual foundations. *2nd Scandinavian Workshop on e-Government*, 1(October 2003), pp.1–20. Available at: http://www.vits.org/publikationer/dokument/492.pdf.

Pettypiece, S., 2017. Trump Lays Groundwork for Federal Government Reorganization. Available at: https://www.bloomberg.com/news/articles/2017-04-12/trump-lays-groundwork-for-widespread-government-reorganization.

Pirsig, R. M. (1974) *Zen and the Art of Motorcycle Maintenance*. William Morrow.

Pittas, N., Jones, A. C. and Gray, W. A. 2001. 'Evolution support in large-scale interoperable systems: a metadata driven approach.', *ADC '01: Proceedings of the 12th Australasian database conference*, pp. 161–168. doi: 10.1109/ADC.2001.904479.

Popper, S. et al., 2004. *System-of-Systems Symposium: Report on a Summer Conversation*, Arlington, VA.

Porlier, M.-J., 2014. Legacy system: A Simple Definition. Available at: https://www.kohezion.com/blog/legacy-system-a-simple-definition/.

Porzel, R. and Malaka, R. (2004) 'A Task-based Approach for Ontology Evaluation'.

Pressman, R. S. (2001) 'Software Engineering A Practitioner's Approach,'.

Pring, R., 2004. *Philosophy of Educational Research*,

Proctor, P.E., Hunter, R. & Mckibben, D., 2008. A Simple IT Risk Management Process. , (September).

Profitt, T., 2008. *Creating a Comprehensive Vulnerability Assessment Program for a Large Company Using QualysGuard*,

Protege 2005. *The protégé ontology editor and knowledge acquisition system*. Available at: http://protege.stanford.edu/.

Prowle, M.,2012. *Mergers of public sector organisations: Not a panacea for austerity!* Available at: http://www.malcolmprowle.com/2012/11/mergers-of-public-sector-organisations.html (Accessed: 15 August 2016).

Public Governance and Territorial Development Directorate, 2014. Recommendation of the Council on Digital Government Strategies.

PWC, 2016. The impact of Brexit on government and public sector. Available at: http://www.pwc.co.uk/the-eu-referendum/the-impact-of-brexit-on-government-and-public-sector.html [Accessed July 5, 2017].

PWC, 2015. 'To own or not to own: Realising the value of public sector assets'.

PWC, 2012. 'Transforming the citizen experience: One Stop Shop for public services', (February). Qualys, 2008. *Vulnerability Management for Dummies*, John Wiley and Sons Limited.

Qualys, 2008. *Vulnerability Management for Dummies*, John Wiley and Sons Limited.

Ragheb, M.,2017. 'Natural disasters and man made accidents ©'.

Rahman, M., 2013. 'Search Engines going beyond Keyword Search: A Survey.', *International Journal of Computer Applications*, 75(17), pp. 1–8. doi: 10.5120/13200-0357.

Raleigh, S. E. H., 2015. *Proposed Expansion of E-Verify Services and Obligations Could Add New Burdens for Employers*. Available at: http://www.ogletreedeakins.com/shared-content/content/blog/2015/august/proposed-expansion-of-everify-services-and-obligations-could-add-new-burdens-for-employers (Accessed: 9 August 2016).
Ramberg, B. & Gjesdal, K., 2005. Hermeneutics. Available at: https://plato.stanford.edu/archives/sum2009/entries/hermeneutics/.

Ravindranath, M., 2016. Why agile is still so hard for the government. Available at: http://www.nextgov.com/emerging-tech/2016/08/government-has-way-go-agile/131034/.

Ray, S., 2017. Guide to Using a Risk Register. Available at: https://www.projectmanager.com/blog/guide-using-risk-register.

Rector, A., 2012. Axioms & Templates : Distinctions & Transformations amongst Ontologies , Frames , & Information Models. , 44(July).

Redman, T. et al., 2007. Evaluating the human resource shared services model: Evidence from the NHS. *The International Journal of Human Resource Managemen*, 18(8), pp.1486–1506.

Reiss, G., 2007. *Project Management Demystified*,

Ren, Y. *et al.*,2014. 'Towards Competency Question-driven Ontology Authoring'.

Repa, V., 2015. Life Events: A Crucial Point of e-Government. In R. Matulevičius & M. Dumas, eds. *Perspectives in Business Informatics Research: 14th International Conference, BIR 2015, Tartu, Estonia, August 26-28, 2015, Proceedings*. Cham: Springer International Publishing, pp. 33–47. Available at: https://doi.org/10.1007/978-3-319-21915-8_3.

Resnik, D.B., 2015. What is Ethics in Research & Why is it Important?

ReSPA, 2015. *E-Government Analysis : From E- to Open Government*,

Reynolds, R., 2014. *Action 2 case study: redesigning services*, Available at: https://www.gov.uk/government/publications/case-study-on-action-2-redesigning-services/action-2-case-study-redesigning-services--2.

Richardson, D. & Patana, P., 2012. Integrating service delivery: Why, For who, and How? , (November), pp.1–28.

Rinaldi, S.M., Peerenboom, J.P. & Kelly, T.K., 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), pp.11–25.

Robert, B. et al., 2003. Characterization and ranking of links connecting life support networks. *Public safety and emergency preparedness*.

Robey, D., Ross, J.W. & Boudreau, M.C., 2002. Learning to implement enterprise systems: An exploratory study of the dialectics of change. *Journal of Management Information Systems*, 19(1), pp.17–46.

Robin, C.R.R. & Uma, G. V, 2011. Design and Development of Ontology for Risk Management in Software Project Management. , 1(Isccc 2009), pp.253–257.

Rolia, J. et al., 2006. Supporting application quality of service in shared resource pools. *Communications of the ACM*, 49(3), pp.55–60.

Rome, E. et al., 2009. DIESIS: An interoperable european federated simulation network for critical infrastructures. *SISO European Simulation Interoperability Workshop 2009, EURO SIW 2009*, (April 2016), pp.137–144. Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-

84865443817&partnerID=tZOtx3y1.

Ron Davies, 2015. eGovernment using technology to improve public services and democratic participation. *September*, (September), p.28.

Rosen, E., 2010. Smashing Silos.

Rouse, M., 2011. loose coupling. Available at: http://searchnetworking.techtarget.com/definition/loose-coupling.

Roux, H. Le, 2016. Breaking down our habitual silos in primary care. Available at: https://www.england.nhs.uk/signuptosafety/2016/04/11/dr-hein-le-roux-3/.

Roy, D., Reuse of Open Government Data.

RSA, N.T., 2004. Asset Management Framework v3.3 2004.

RSM, 2016. Police risk register analysis. , (November).

RWJF, 2008. Collecting Texts and Artifacts.

Sabol, T., Furd'ik, K. & Mach, M., 2010. Semantic Technologies for E-Government. In T. Vitvar, V. Peristeras, & K. Tarabanis, eds. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 47–74. Available at: http://dx.doi.org/10.1007/978-3-642-03507-4_3.

Saffin, T. & Laryea, S., 2012. THE USE OF RISK REGISTERS BY PROJECT MANAGERS. , (July), pp.1307–1320.

Saftawy, A., 2015. What is "Hard" and "Soft" Infrastructure? Available at: https://www.linkedin.com/pulse/what-hard-soft-infrastructure-ahmed-saftawy.

Sage, A.P. & Cuppan, C.D., 2001. On the Systems Engineering and Management of Systems of Systems and Federations of Systems. *Inf. Knowl. Syst. Manag.*, 2(4), pp.325–345. Available at: http://dl.acm.org/citation.cfm?id=1234195.1234200\nhttp://datafedwiki.wustl.edu/images/7/7a/Sage-On_the_Systems_Engineering_and_Management_of_Systems_of_Systems.pdf.

Sahay, A.A., 2016. Peeling Saunder ' s Research Onion. , (October).

Saleh, Z.I., Obeidat, R.A. & Khamayseh, Y., 2013. A Framework for an E-government Based on Service Oriented Architecture for Jordan. *I.J. Information Engineering and Electronic Business*, (September), pp.1–10.

Samarin, A., 2014. E-government reference model.

Sanati, F. & Lu, J., 2007. A Methodological Framework for E-government Service Delivery Integration. , pp.1–9.

Sanjari, M. et al., 2014. Journal of Medical Ethics and History of Medicine E thical challenges of researchers in qualitative studies : the necessity to develop a specific guideline. , pp.1–6.

SAPM, 2014. Too Slow! Government IT project lacks Agility. Available at: https://blog.inf.ed.ac.uk/sapm/2014/02/14/too-slow-government-it-project-lacks-agility/.

Saran, C., 2004. Integration of legacy systems is vital to effective customer service. Available at: http://www.computerweekly.com/feature/Integration-of-legacy-systems-is-vital-to-effective-customer-service.

Sarikas, O.D. & Weerakkody, V., 2007. Realising integrated e-government services: a UK local government perspective. *Transforming Government: People, Process and Policy*, 1(2), pp.153–173. Available at: http://dx.doi.org/10.1108/17506160710751986.

Saunders, M., Lewis, P. & Thornhill, A., 2012. *Research Methods for Business Students* 6th ed., Pearson.

Saunders, M.N. & Rojon, C., 2014. There ' s no madness in my method : Explaining how your research findings are built on firm foundations.

Saunders, B. M. and Tosey, P., 2012. 'The Layers of Research Design'.

Saunders, M.N.K., 2012. Choosing research participants. In G. Symon & C. Cassell, eds. *The practice of qualitative organizational research: Core methods and current challenges*. London: SAGE Publications Inc, pp. 37–55.

Sauro, J., 2015. 5 Types of Qualitative Methods. Available at: https://measuringu.com/qual-methods/.

Schulman, J. & Baum, C.H., 2003. The Gartner Enterprise Architecture for Government.

Schulz, V. et al., 2009. Definition and classification of IT-shared-service-center. In *Americas Conference on Information Systems*. pp. 1–11.

Schwandt, T., 2000. Three epistemological stances for qualitative inquiry.

Segarra, J., 2016. Three ways workflow automation helps government agencies. Available at: http://whatsnext.nuance.com/office-productivity/three-ways-workflow-automation-helps-government-agencies/.

Seifert, J.W., 2003. A Primer on E-Government : Sectors, Stages, Opportunities, and Challenges of Online Governance. *Report for Congress*, p.24.

Semantic Web, 2007. OTK methodology. Available at: http://semanticweb.org/wiki/OTK_methodology.html.

Serrano, N., Hernantes, J. & Gallardo, G., 2015. Service-Oriented Architecture and Legacy Systems. Available at: https://www.infoq.com/articles/service-oriented-architecture-and-legacy-systems/#.

Service Futures, 2015. One of the most needed optimization efforts in the public sector? Breaking the organizational silos. Available at: https://servicefutures.com/integrated-facility-services/one-needed-optimization-efforts-public-sector-breaking-organizational-silos/ [Accessed July 30, 2017].

Service Manual UK, 2016. *Moving away from legacy systems*, Available at: https://www.gov.uk/service-manual/technology/moving-away-from-legacy-systems.

Shah, H. *et al.*, 2015 'A Survey Of Ontology Evaluation Techniques For Data Retrieval', 4(11), pp. 14960–14962. doi: 10.18535/Ijecs/v4i.

Sheng, L. & Lingling, L., 2011. Application of Ontology in E-Government. *2011 Fifth International Conference on Management of e-Commerce and e-Government*, pp.93–96. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6092638 [Accessed April 22, 2014].

Sherif, M.H., 2010. Defining Systems Integration. In M. H. Sherif, ed. *Handbook of Enterprise Integration*. Taylor and Francis Group LLC.

Da Silva, L.É.P. et al., 2014. ONTO-ResAsset development: An ontology for reusable assets specification and management. *Proceedings of the International Conference on Software Engineering and Knowledge Engineering, SEKE*, 2014-Janua(January), pp.459–462. Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84938366478&partnerID=tZOtx3y1.

Silva, W.B. e, 2017. Infrastructure gap: What does it mean for public policy makers? Available at: https://www.linkedin.com/pulse/infrastructure-gap-what-does-mean-public-policy-willian-bueno-e-silva.

Simon, H.A., 1996. *The Sciences of the Artificial Third edition*,

Singh, S., 2015. ‘e-Government: Institutional and environmental challenges’, *Proceedings of the 7th International Conference on Business and Finance*, pp. 1–7. doi: 10.4102/jbmd.v5i1.4.

Singhal, A. & Singapogu, S., 2012. Security Ontologies for Modeling Enterprise Level Risk Assessment.

Singleton, F., 2015. Government as a platform for the rest of us. Available at: https://gds.blog.gov.uk/2015/10/07/government-as-a-platform-for-the-rest-of-us/.

Sirin, E. *et al.*, 2007. ‘Pellet: A practical OWL-DL reasoner’, *Web Semantics*, 5(2), pp. 51–53. doi: 10.1016/j.websem.2007.03.004.

Sofaer, S., 2002. Qualitative Research Methods. *Methodology Matters*.

Sohal, A.S. & Fitzpatrick, P., 2002. IT governance and management in large Australian organisations. , 75, pp.97–112.

Sommerville, I., 2000. 26 . Legacy Systems. , pp.1–22.

Sommerville, I., 2004. ‘Software evolution’, pp. 1–47.

Soy, S., 1997. *The Case Study as a Research Method*. Available at: https://www.ischool.utexas.edu/~ssoy/usesusers/l391d1b.htm.

Steele, A., 2008. Ontological Vulnerability Assessment. In S. Hartmann, X. Zhou, & M. Kirchberg, eds. *Web Information Systems Engineering – WISE 2008 Workshops*. Springer Berlin Heidelberg, pp. 24–35.

Sterman, J. D., 2012. *Sustaining Sustainability : Creating a Systems Science in a Fragmented Academy and Polarized World*. doi: 10.1007/978-1-4614-3188-6.

Strammiello, C., 2016. 3 steps to streamlining government workflows. Available at: https://gcn.com/articles/2016/03/02/electronic-document-workflow.aspx.

Strauss, A. & Corbin, J., 1994. Grounded Tehory Methodology.

Sue Greener, 2008. *Business Research Methods*,

Sunagawa, E. et al., 2003. Management of dependency between two or more ontologies in an environment for distributed development.

Suter, E. et al., 2009. Ten Key Principles for Successful Health Systems Integration. *Healthcare quarterly (Toronto, Ont.)*, 13(Spec No), pp.16–23. Available at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3004930/.

Svensson, J., 2016. 7 Reasons to Replace Your ERP System.

Syal, R., 2014. Ministry of Justice writes off £56m on duplicate IT project. *The Guardian*. Available at: https://www.theguardian.com/politics/2014/jun/29/ministry-justice-56m-writeoff-it-project.

Syalim, A., Hori, Y. & Sakurai, K., 2009. Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft’s Security Management Guide. In *ARES 2009*. pp. 726–731.

Tambouris, E. et al., 2004. Ontology-enabled e-Gov Service Configuration : An Overview of the OntoGov project State of the Art and Related Projects.

Tambouris, E., Manouselis, N. & Costopoulou, C., 2007. Metadata for digital collections of e-government resources M. Sicilia, ed. *The Electronic Library*, 25(2), pp.176–192. Available at: http://www.emeraldinsight.com/doi/abs/10.1108/02640470710741313 [Accessed October 15, 2015].

Telegraph View, 2015. Our legal system is dysfunctional and must be reformed. Available at: http://www.telegraph.co.uk/news/uknews/law-and-order/11694744/Our-legal-system-is-dysfunctional-and-

must-be-reformed.html.

Tett, G., 2016. *The Silo Effect: The Peril of Expertise and the Promise of Breaking Down Barriers*, Simon & Schuster.

Tett, G., 2015. *The Silo Effect: Why putting everything in its place isn't such a bright idea*, Little, Brown.

The Institute of Internal Auditors, 2014. Managing Third-party Risks. , (67), pp.1–4.

The MITRE Corporation, Common Vulnerabilities and Exposures. Available at: http://cve.mitre.org/ [Accessed July 30, 2016].

The National Archives, 2017. Identifying Information Assets and Business Requirements. Available at: http://www.nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf.

The White House, O. of the P.S., 2012. Government Reorganization Fact Sheet. Available at: https://obamawhitehouse.archives.gov/the-press-office/2012/01/13/government-reorganization-fact-sheet.

The World Bank, 2014. Innovative Technologies to Help County Governments Improve Service Delivery. Available at: http://www.worldbank.org/en/news/press-release/2014/03/26/innovative-technologies-to-help-county-governments-improve-service-delivery.

Thomas, R. & Walport, M., 2008. Data Sharing Review Report. , (July).

Thomson Reuters, 2013. Emerging legal technologies and workflow challenges facing public law offices White paper.

Tibbetts, H., 2012. Legacy Modernization, Integration & Agility. Available at: http://www.ebizq.net/blogs/integrationedge/2012/05/legacy-modernization-integration-agility.php.

Todorovski, L. et al., 2006. Methodology for Building Models of Life Events for Active Portals. *Communication Proceedings of the Fifth International EGOV Conference*, (August 2016), pp.61–68.

Todorovski, L. et al., 2007. OneStopGov: D12 - Life-event Analysis and Description Language.

Todorovski, L., Kunstelj, M. & Vintar, M., 2007. Reference Models for E-Services Integration Based on Life-Events. In M. A. Wimmer, J. Scholl, & Å. Grönlund, eds. *Electronic Government: 6th International Conference, EGOV 2007, Regensburg, Germany, September 3-7, 2007. Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 92–103. Available at: http://dx.doi.org/10.1007/978-3-540-74444-3_9.

Tohidi, H., 2011. Procedia Computer E-government and its different dimensions : Iran. *Procedia Computer Science*, 3, pp.1101–1105. Available at: http://dx.doi.org/10.1016/j.procs.2010.12.179.

Topping, A., 2015. Children trapped in poverty by UK government's "dysfunctional system." Available at: https://www.theguardian.com/society/2015/jun/03/no-recourse-to-public-funds-children-poverty-uk-government.

Traunmüller, R. & M. Wimmer, 2001. Directions in E-Government: Processes, Portals, Knowledge. In *Proceedings of the 12th International Workshop on Database and Expert Systems Applications*. Washington, DC, pp. 313–317.

Trochidis, I., Tambouris, E. & Tarabanis, K., 2006. Identifying Common Workflow Patterns in Life-Events and Business Episodes. In *International Conference on E-Government*.

Tsoumas, B. & Gritzalis, D., 2006. Towards an ontology-based security management. *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, 1, pp.985–990.

U.S. Department of Transportation & Administration, F.H., 2010. Data Integration Primer. , (august).

UK Government Cabinet Office, 2014. D5 Charter. , pp.5–6.

UK Government Cabinet Office, 2013. Integration across government. , (March).

Ullman, J.D., 2000. Information integration using logical views.

Ulrich, D., 1995. Shared services: From vogue to value. *Human Resource Planning*, 18(3), pp.12–23.

United Nations and American Society for Public Administration, 2001. Global Survey of E-government.

United Nations E-Government Survey, 2014. World e-government rankings.

Uschold, M. and Gruninger, M., 1996. 'Ontologies: Principles Methods and Applications', *Knowledge Engineering Review*, 11(2), pp. 1–63.

Uschold, M., 2004. Ontologies and Semantics for Seamless Connectivity ‡ 1 Introduction. , 33(4), pp.58–64.

Uschold, M. et al., 1998. The Enterprise Ontology. *The Knowledge Engineering Review*, 13(1 Special Issue on Putting Ontologies to Use), pp.31–89.

Uschold, M. & Gruninger, M., 1996. Ontologies: Principles Methods and Applications. *Knowledge Engineering Review*, 11(2), pp.1–63.

Uschold, M. & Jasper, R., 1999. A Framework for Understanding and Classifying Ontology Applications. , pp.1–12.

Uschold, M. & King, M., 1995. Towards a Methodology for Building Ontologies conjunction with IJCAI-95 Abstract. , (July).

Vaishnavi, V. & Kuechler, B., 2015. Design Science Research in Information Systems Overview of Design Science Research.

Valayer, C., 2014. GOVERNANCE MODELS FOR SHARING AND RE-USE FOR COMMON IT SOLUTIONS. , pp.1–45.

Vale, R., 2017. Prison Register goes into alpha. Available at: https://mojdigital.blog.gov.uk/2017/03/27/guest-post-prison-register-goes-into-alpha/ [Accessed July 24, 2017].

Vassilakis, C. & Lepouras, G., 2006. Ontology for E-Government Public Services.

Vaus, D. De, 2001. Research Design in Social Research.

VersionOne, 2016. 10th Annual Stage of agile report.

VersionOne, 2017. The 11th Annual State of Agile Report.

VersionOne, 2015. The 9th Annual State of Agile Report. Available at: http://info.versionone.com/state-of-agile-development-survey-ninth.

Voort, H. van der, Bruijn, H. de & Janssen, M., 2009. Transformation Strategies for Shared Service Centers in the Public Sector. , pp.35–37.

Vrande, D. *et al.*, 2010. 'Ontology Evaluation', (June).

W3C, 2009a. Improving Access to Government through Better Use of the Web. Available at: https://www.w3.org/TR/egov-improving/.

W3C, 2004a. OWL Web ontology language use cases and requirements. Available at: http://www.w3.org/TR/webont-req/ [Accessed September 21, 2015].

W3C, 2009b. Semantic Web. Available at: http://www.w3.org/RDF/FAQ [Accessed October 8, 2015].

W3C, 2004b. Web Services Glossary. *W3C Working Group Note*. Available at: http://www.w3.org/TR/ws-gloss/ [Accessed August 4, 2016].

Waddock, S., 2013. Thinking about Large Scale System Change.

Wallace, W.A. et al., 2003. Managing Disruptions to Critical Interdependent Infrastructures in the Context of the 2001 World Trade Center Attack. In *Natural Hazards Research and Applications*. Colorado, pp. 165–198.

Walsh, N., 2016a. The leadership challenges of sustainability and transformation plans. Available at: https://www.kingsfund.org.uk/blog/2016/04/leadership-challenges-stps.

Walsh, N., 2016b. Will STPs deliver the changes we wish to see in our health and care services? Available at: https://www.kingsfund.org.uk/blog/2016/11/will-stps-deliver-changes-we-wish-see-our-health-and-care-services.

Walsham, G., 2013. Development Informatics in a Changing World : Reflections from ICTD2010 / 2012. , 9(1), pp.49–54.

Wang, J. & Guo, M., 2009. OVM: an ontology for vulnerability management. *Proceedings of the 5th Annual Workshop on Cyber …*, pp.1–4. Available at: http://150.254.220.12/han/ACMLibrary/delivery.acm.org/10.1145/1560000/1558646/a34-wang-slides.pdf?ip=150.254.220.12&id=1558646&acc=ACTIVE SERVICE&key=6AF5E6E07E3D4A13.3C6032F2CFB81A51.4D4702B0C3E38B35.4D4702B0C3E38B35 &CFID=424456708&CFTOKEN=64356138.

Wang, J., Guo, M.M. & Camargo, J., 2010. An Ontological Approach to Computer System Security. *Information Security Journal: A Global Perspective*, 19(2), pp.61–73. Available at: http://www.tandfonline.com/doi/abs/10.1080/19393550903404902.

Wang, S., Shen, W. & Hao, Q., 2006. An agent-based Web service workflow model for inter-enterprise collaboration. *Expert Systems with Applications*, 31(4), pp.787–799.

Warren, P.D., Varney, R.M. & Horwath, C., 2014. Third-Party Risk and What to Do About It. Available at: http://www.industryweek.com/supplier-relationships/third-party-risk-and-what-do-about-it.

Washington Examiner, 2017. These 8 federal agencies are the worst. Here's how to fix them. Available at: http://www.washingtonexaminer.com/these-8-federal-agencies-are-the-worst-heres-how-to-fix-them/article/2583708.

Watts, S., 2017. COBIT vs ITIL: Understanding IT Governance Frameworks. Available at: http://www.bmc.com/blogs/cobit-vs-itil-understanding-governance-frameworks/.

Webb, A., 2003. *The project Manager's Guide to Handling Risk*,

Webster, D. W. and Stanton, T. H., 2015. 'Improving Government Decision Making through Enterprise Risk Management Improving Government Decision Making through Enterprise Risk Management', pp. 1–31.

Weerakkody, V., Janssen, M. & Dwivedi, Y.K., 2009. *Handbook of Research on ICT-Enabled Transformational Government: A Global Perspective*, IGI Global.

Weldring, T., 2016. "Not another piece of paper!" – from silos to whole system thinking. Available at: https://www.england.nhs.uk/signuptosafety/2016/06/30/theresa-weldring/.

Weller, S. 2015. 'The potentials and pitfalls of using Skype for qualitative (longitudinal) interviews'.

Welsh Government news, 2015. Home About Us What We Do Our Members Events Media & Resources Contact £6.7m investment in new IT system to integrate NHS and social services in Wales. Available at: http://www.adsscymru.org.uk/media-resources-list/6-7m-investment-in-new-it-system-to-integrate-nhs-and-social-services-in-wales/.

Wen-fei, G.A.O. & Xin-li, Z., 2008. Constructing the Relationship between Concepts in Government Ontology Based on E-Government Thesauri construction of ontology in China concepts in government ontology based on the E-government Thesaurus. , (70573103), pp.116–121.

West, D., 2016. Government projects are not agile enough. Available at: https://fcw.com/articles/2016/06/23/comment-west-agile.aspx.

West, D.M., 2008. Improving Technology Utilization in Electronic Government around the World, 2008. Available at: https://www.brookings.edu/research/improving-technology-utilization-in-electronic-government-around-the-world-2008/.

Whitman, M. & Mattord, H., 2014. *Principles of Information Security*, Course Technology.

Wickramasinghe, N. et al., 2007. Healthcare System of Systems. *2007 IEEE International Conference on System of Systems Engineering*, pp.1–6. Available at: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4304283.

Williams, T.M., 1996. The two-dimensionality of project risk. , 14(3), pp.185–186.

Wilson, S. et al., 2016. Joining up public services around local , citizen needs.

Winter, B.R. & Fischer, R., 2007. Article Essential Layers , Artifacts , and Dependencies of Enterprise Architecture. , (May), pp.1–12.

Wirth, T. & Smith, R., 2016. GOV.UK Pay gets Payment Card Industry (PCI) accreditation.

Wolstencroft, K. . *et al.*, 2011. 'RightField: embedding ontology annotation in spreadsheets'.

Worley, D., 2015. Digital take up- Its not just channel shift.

Wyman, O., 2009. OECD Studies in Risk Management INNOVATION IN COUNTRY.

Yin, R.., 2009. Case Study Research : design and methods .

Yusta, J.M., Correa, G.J. & Lacal-Ar??ntegui, R., 2011. Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy*, 39(10), pp.6100–6119.

Zhang, P. & Peeta, S., 2011. A generalized modeling framework to analyze interdependencies among infrastructure systems. *Transportation Research part B: Methodological*, 45(3), pp.553–579.

Zhang, P., Scialdone, M. & Ku, M.-C., 2011. IT Artifacts and The State of IS Research. In *IT Artifacts and The State of IS Research*.

Zhao, J. et al., 2012. Why Workflows Break - Understanding and Combating Decay in Taverna Workflows.

Zhu, H. et al., 2007. An Integrated Model in E-Government Based on Semantic Web , Web Service and Intelligent Agent.

Zimmerman, R., 2001. Social implications of infrastructure network interactions. *Journal of Urban Technology*, 8, pp.97–119.

Zukauskas, H. D. P. and Kasteckiene, A., 2002. 'The Role of E-Government in the Development of the New Economy in Lithuania'.

Appendices

Appendix I: Publication

Development of an E-Government Ontology to Support Risk Analysis

Onyekachi Onwudike, Russell Lock, Iain Phillips

Department of Computer Science, Loughborough University

o.c.onwudike@lboro.ac.uk r.lock@lboro.ac.uk i.w.phillips@lboro.ac.uk

Abstract: The complexity of governments is one of the biggest problems citizens face in engaging with them. This complexity is seen in the growing number of departments and services that a government is made up of and the need for citizens to interact with these departments or services independently. This research shows a lack of efficiency in the E-Government domain due to the vertical alignment of services and the need for complex collaboration across the departments, which all too often does not exist. We propose that an ontology could potentially help to foster interactions between departments and services, and thereby manage this complexity more efficiently. Although ontologies exist for different subject domains, the quality and suitability of these ontologies in the government domain at the present time gives rise for concern. Ontologies have the potential to play an important role in the design and development of government services. The key reason behind the development and design of an ontology for the E-Government domain is to use knowledge that is resident in the domain of governments to reduce risks associated with the delivery, combination and dependencies that exist amongst services so that the resilience of the E-Government domain can be improved throughout government. This paper addresses the issue of identifying and analysing risk in the development and deployment of E-Government services. Relevant information on risks that may occur with respect to services can be collected, compiled and disseminated which can serve as prediction tools for future governments as well as enable service providers make choices that would enable them fulfil service requirements adequately. The aim of this research is to contribute by constructing an ontology that is aimed at gauging the risks associated with using solutions across departments and even governments. Further, we also document how we have made use of queries to validate this ontology.

Keywords: E-Government, Ontology, Relationships, Reuse, Risks.

1. Introduction

As a working approximation the average government is made up of around 50-80 different departments and agencies. For matters that are as simple as registering the birth of a child, different agencies and departments require a bewildering array of information often inputted in different ways, into different systems, and stored/accessed in multiple locations. Rather than these departments communicating amongst themselves, they expect citizens to communicate with them individually. One solution to the problems faced by governments is the use of ontologies. The reasons for building E-Government ontologies are many and varied. They include but are not limited to the following:

1. To create and distribute information;
2. To maintain information on data and its usage adequately;
3. To enforce standards in the way data is exchanged;
4. To aggregate data with the use of languages such as OWL;
5. To interpret data formally with the use of semantics and to adequately control 6. vocabularies;
6. To emphasize trust in data sources because there is provenance of information;
7. To compare and correlate data;
8. To make government efficiencies and effectiveness transparent; and
9. To make sure there is accountability in the process of making policies.

Sowa (Sowa 2000) defined an ontology as a discipline that forms part of the field of knowledge representation. Ontologies are commonly applied to model information from different application domains in order to support analysis. They can be used in the representation of services governments offer to her citizens as well as in supporting the providers of these services in the delivery of these services, and the receivers of these services in accessing the availability of services to them in a structured and logical way. Different E-Government ontologies have been developed for different strata of government in the past; however, these ontologies have had little or no impact on E-Government as a whole arguably due to the lack of collaboration that has taken place during construction, and due to the inherent lack of collaborative support built into them by the developers. Therefore, the ontology this paper presents has been explicitly designed to improve collaboration and

has been formulated using real world data. Although the idea of reuse across ontologies seems to be a welcome idea with respect to the problem of interoperability, the risks and disadvantages associated with reusing existing solutions, as well as making certain functionalities shareable between E-Government services is a concern. We explore the use of ontologies in overcoming risks associated with reusing solutions developed for one department in another department and conclude, with the support of case studies for evaluation, that the use of ontologies could be beneficial in gauging the risks associated with this. This theory is supported by a case study which highlights what can be achieved through reasoning with an OWL ontology extended appropriately by rules. The application aims at modelling the definition of risks that may be identified in the combination of services in the E-Government domain. Simplified examples are provided in the paper to illustrate why OWL needs to be supplemented with rules for reasoning over hybrid knowledge and potential issues with doing so are discussed. The development of a suitably designed ontology could add value to the E-Government domain in areas of modelling relationships that exist between Departments and services as well as in overcoming the risks associated with reusing solutions across departments in government. Therefore, the role of the research and the artefact created in the form of an ontology is to educate governments and the providers of services so that risks can be reduced as well as the resilience of the system increased. The rest of the paper is structured as follows: Section two elaborates on existing E-Government ontologies; Section three presents application contexts where a suitably designed ontology can be used to gauge risks in the E-Government domain; Section four makes use of instances of the E-Government ontology to present cases for its relevance and finally Section five presents the conclusions, limitations and potential of this novel approach.

2. E-Government Ontologies

In terms of the sharing of knowledge, an ontology is defined as an explicit specification of a conceptualisation (Gruber 1993). In computing, an ontology can be likened to a framework used for the representation of concepts (things, or ideas about things) and the relationships that exist between those concepts (Uschold & Gruninger 1996). Therefore, an ontology is aimed at modelling only those entities and relationships deemed relevant within a particular domain. An E-Government ontology can be defined as an explicit description of the E-Government domain containing a common vocabulary to support shared understanding between users. Concepts and relations managed by any scientific community can benefit

from formal definitions and the use of ontologies is one of the key ways to achieve this. Several E-Government ontologies have been developed in the past, including SmartGov, EGov, OntoGov, TerreGov etc. While the OntoGov ontology focussed on making electronic services interoperable and accessible to people all over the globe it lacked the ability to specify roles and actors in the development of the ontology as well as the ability to logically make queries. The SmartGov ontology was designed with the intention of helping public authorities overcome barriers in planning, designing, and delivery of electronic services, but fell short because it was difficult to establish concepts that were related to E-Government in the ontology. Although the TerreGov ontology dealt with interoperability issues of E-Government services for local and regional governments there was an absence of focus for a global community. The EGov ontology encouraged a onestop government and provided information to citizens but lacked the ability to define complex concepts and relationships; The focus of the QUALEG and QUONTO ontologies was on the problem of integrating services but failed to establish interaction between government and her citizens. Therefore, citizens perception of government services were ignored. The question therefore arises, why are the ontologies previously developed not being applied today? Although there was an attempt by these ontologies to address varying problems in the E-Government domain, (Gugliotta A et al. 2005) argue that not one of these ontologies embraces Semantic Web technologies to represent concepts and actions. Many of these ontologies are already obsolete and more crucially lack semantic consistency in their design which has led to loss of critical information. Despite this, ontology development for E-Government is an area that has received considerable interest. According to (Fonou-dombeu & Huisman 2011), ontologies are used to describe and specify E-Government services (E-services), primarily because semantic integration and interoperability of E- services are facilitated with their use; there is ease in composition, matching, mapping and merging of various E-Government services. Therefore, the purpose of the E-Government ontology is to facilitate adequate understanding of the E-Government domain by service providers so that issues relating to the integration of services as well as the risks associated with integration in the Government domain can be addressed, as well as used as prediction tools for future governments. It is extremely difficult to develop a single ontology that satisfies all users especially in the areas of precision, coverage, actuality and individualization. This can be attributed to the fact that specific approaches as well as vocabularies are needed by different departments for solving tasks specific to them (Stumme et al. 2000). The development of E-Government ontologies in isolation, without wider integration in perspective and the lack of reuse of components

present serious challenges for the E-Government domain. Ontologies serve as a platform or a means for defining the services offered by governments and attempts have been made at the development of E-Government ontologies. The use of ontologies for knowledge representation can enhance organizational communication and re-usability and serve as the building blocks for intelligent systems. To the best of our knowledge, there is no directly related work focussed on the development of an E-Government ontology to gauge risks associated with E-Government services. The focus of other related work have been on the development of semantic driven government (Fonou-dombeu & Huisman 2011). (Gugliotta et al. 2005) focussed on the development of E-Government portals and (Sheng & Lingling 2011) focussed on the application of ontology in E-Government.

2.1 Method of Development

To develop the E-Government ontology used in this paper, the steps provided by (Noy & McGuinness 2001) were followed with emphasis on the repetitive process stated in it. This method of ontology development as proposed by (Noy & McGuinness 2001) was used because it is an increasingly popular method for organizing information and has successfully been used in the past by other ontology developers. The process involved determining the scope and domain of the ontology which involved sketching a list of questions the ontology should be able to answer referred to as competency questions; enumerating important terms and relationships; definition of classes and subclasses as well as formulating a class hierarchy; definition of class properties as well as their cardinalities and values and creating instances in the ontology. The competency questions are focussed on what we intend the ontology to do and what questions the ontology should be able to address. With the help of the competency questions we were able to formalise a scope for the ontology which aided the enumeration of important terms and enabled us to define the class structure of the ontology. The key competency questions that were considered during the development of the ontology include but are not limited to the following:

1. What services are available to a citizen?
2. What service is characteristic of a department?
3. What services can be combined?
4. What are the criteria for combining services?
5. What happens if services that are combined fail?

Based on this list of questions, the ontology will include the information on various services, departments and their characteristics. The design of the ontology was carried out generically so that it could be used to support reuse across governments globally. A large number of related terms were gathered from existing publicly available documentation with the most general and most important of them forming the classes; some of them were used to form properties and others were not used at all because their relevance in the ontology could not be ascertained. Development of the classes and the corresponding class hierarchy formed the next stage of the process. Considering that different approaches can be used in developing the class hierarchy which are the top-down approach, the bottom-up approach and a combination of the two approaches we made use of a combination of the two approaches. In response to the competency questions, we made use of a combination of both approaches because the top-down approach was best suited which gave a well-defined class hierarchy and then the remaining concepts were incorporated into the ontology with the bottom-up approach. The development of the class hierarchy paved the way for definition of class and objects properties which included defining values, value types and their cardinalities. In order to highlight different scenarios of risks, we made use of the UK Government website as our source of data because it contains semi-structured data and because of the mode of storage of data. The UK Government is one that works with devolved ministries, emergency responders and other organisations which enables the UK government to prepare for, respond to and recover from risks it is faced with. Therefore, in order to achieve this, there has to be a preparation and readiness to deal with risks and emergencies not just from the stakeholders' point of view but also in terms of the flexibility of an ontology to support the evolving nature of services and situations. We defined services in terms of other services they were dependent on; departments in terms of departments they were dependent on and were able to model and analyse situations where a given department were critically dependent on another for systems leading to potential shared points of failure. A typical example of departments being dependent on other departments included in our ontology from the UK Gov website is the Attorney General's Office which is a Ministerial department that works with three Non-Ministerial Departments (Crown Prosecution Service, Serious Fraud Office and the Treasury Solicitors Office) and an agency (HM Crown Prosecution Service Inspectorate). Based on the way the UK Government has been structured, it is clear that certain departments cannot function without some other departments or agencies being in place. It also shows that since some departments are overly dependent on other departments, there could be overlooked or incorrectly calculated risks present. This therefore

highlights the need to address actively whether reuse is desirable, and whether the details and potential implications of that reuse are clearly defined within government. In terms of services being dependent on other services but still functioning largely in silos we highlight a scenario based on the UK Benefits Service. Child Benefit is a type of generic Benefit service in terms of our ontology, which itself is represented in this scenario by the creation of a specific instance of that service within the UK government, the Guardians Allowance Service. However, the Guardians Allowance Service is also an instance of the Deaths and Benefits Service which is also a type of Benefit. Other examples include the Carers and Disability Benefit service a type of Benefit service also which shares Carers Credit as an instance with the Job Seekers Allowance service and the Low-Income Benefits service. We see the dependencies between these services and conclude that while these dependencies may have been considered in terms of risk, an ontology would make such a process more efficient by structuring the data logically. In Figure 1 we show a part of the developed ontology hierarchy. The classes of the depicted ontology, i.e. E-Government, Person, Threats etc. and their corresponding subclasses which cover the basic concepts that describe the context of an E-Government application. In terms of the structure of our ontology and to overcome the problems other E-Government ontologies faced which included a surprising lack of semantic consistency and insufficiently defined relationships between the different departments; we developed our structure thus: The set of government services is primarily considered in terms of those users who have a relationship to the services, represented within our ontology by the class Person who can belong to a department and, offer, support or consume services. The structure of our ontology also helped us define relationships beyond the ‘isa’ relationship commonly found in upper level ontologies.

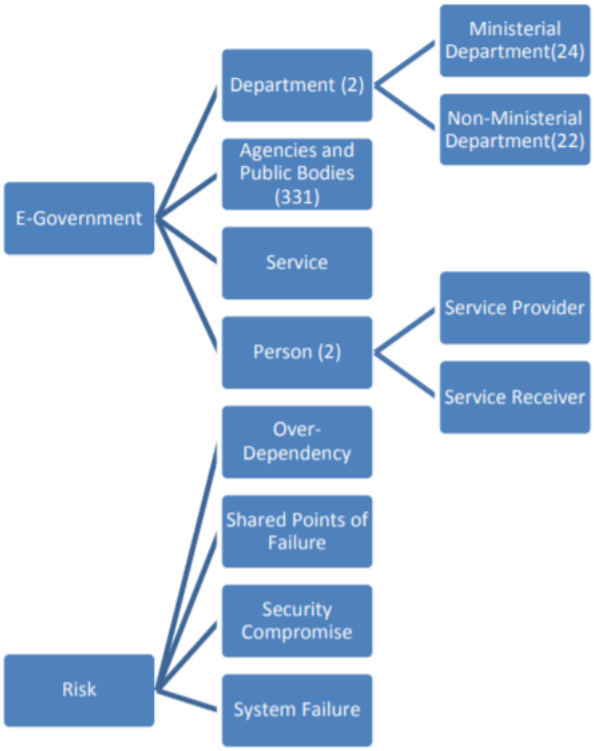


Figure 1: The Ontology Hierarchy

3. Application Scenarios

The purpose of E-Government is to provide services that are focussed on citizens as well as address the demands of citizens and businesses so that they can be accessible, responsive, simple and transparent for the users (Karyda et al. 2006). E-Government services are provided through applications that need to have increased security and privacy features. Although the security and privacy features are key to any government, the possibility of sharing services and reusing solutions across departments and even government cannot be ignored.

3.1 Benefit Service

In this section, we revisit the scenario of a Benefits service running in the UK E-Government domain (www.gov.uk). This service includes the different types of benefits accessible to citizens; when and how benefit payments are made; eligibility for benefits and when it is supposed to stop. The receiver of this service would be able to ascertain whether he is eligible

for a benefit. The benefit issuing authority would be in a position to verify eligibility, make cross-checks and get additional information from the benefit credit facility. Although this process requires confidentiality, privacy and integrity of the entire benefit process; many of the features required are common to other departments or services such as the Births, Deaths, Marriages and care department. However, this scenario can be made up of the following processes but not limited to:

- Management of personal information by users
- Viewing of previous benefits received by users
- Processing of eligibility criteria
- Notification by system that additional information is needed
- Users update additional information required by system with the needed information.

Although in the scenario analysed, major security requirements need to be met such as authentication and authorization of users, this information needs to still be shared across departments requiring this information.

3.2 Births, Deaths and Marriages Service

In this section we present another scenario in the form of the UK Births, Deaths and Marriages service that offers the child benefit service as a subclass and yet has this same service as a type of service in the Benefits service (www.gov.uk). In the development of a Births, Death and Marriage application, this service includes the registration of a birth, death or marriage; eligibility for benefits and when it should stop; dealing with benefits, taxes and leaving care. This shows us that a solution used for the benefits department with respect to eligibility for benefits and when it should be stopped could be reused for the Births, Deaths and marriages department, however, the purpose of the ontology in this respect would be to highlight the risks related to doing so.

4. Using the E-Government Ontology to Gauge Risks

In this section, we illustrate how the E-Government ontology can be used to gauge the risks associated with combining services or even reusing solutions. We also illustrate how the ontology is validated as development of the ontology progresses. We made use of Protégé4.2 for the development of the ontology and queries were run with the Racer reasoner. Protégé 4 is an ontology editor used for creating OWL ontologies. It cannot work without the OWL

API in place. It makes use of a Description Logic Reasoner which checks the consistency of the ontology and automatically computes the ontology class hierarchy. For the purpose of this Research, we made use of OWL-DL which is known to be a more expressive OWL language. It is based on Description Logics which are a component of First Order Logic and are key to automated reasoning. It has the capability of computing the classification hierarchy of an ontology as well as checking for inconsistencies in the ontology (Horridge, 2007). The Racer Reasoner is used for making references and for answering queries over RDF documents (Gmbh 2010). We used it to check for inconsistencies in the ontology and to submit queries so that their validity could be verified. These queries we expressed with the use of the new Racer Query Language (nRQL). The nRQL is a query language that makes use of description logic for retrieving individuals from the Abox which is known as a set of assertions about individuals. This language allows the use of variables which are bound against the individuals in the a-box that satisfy the conditions. Protégé and Racer were able to communicate because of the RQL tab plug-in that was installed. We provide a set of nRQL queries with their answers below illustrating the use of the E-Government ontology to gauge risks associated with reusing solutions.

4.1 Results of nRQL Queries

An ontology is said to be useful when it can give answers that are consistent to real-world questions. In this section, we list a number of questions a service provider is likely to come up with when attempting to reuse solutions in the E-Government domain. Although these questions are not exhaustive, they indicate what the ontology can deal with and what level of reasoning it can cope with. We express each question as an nRQL query and present the result of the executed query. The questions presented in this section also guided us in the development of the ontology while the queries presented were used in validating our ontology.

4.1.1 Questions Associated with Reusing Solutions

Having an understanding of the type of risk that may take place when services are combined or solutions are reused gives us an insight into the conflicts that may take place within the back-office situation especially with respect to sharing of resources and information property rights. (Homburg et al. 2002) analysed the effects of resource dependence theory and information property rights theory stating the conflicts that could stem from such mixtures

in the network. The development of services requires heavy reliance on the use of IT systems. (Woll et al. 2013) outlined a major challenge associated with this as lack of interoperability between different IT systems. Although a lot of research and industrial activities have focused on the feasibility of interoperability in the past, the problem still lingers. (Woll et al. 2013) also outlined how approaches have been mapped out on embracing interoperability but there is a lack of application in the industry. This they attributed to the high cost of linking many different IT systems and the data contained in them. To successfully build a platform for E-Government to operate requires the collation of information from the different departments and parastatals that make up the government. Hence, there is a lot of replicated data as data collated for one department may be the same data collated across other departments even though the modes of collation or delivery may differ. A typical scenario seen while building this ontology from the UK Government website is in the department of Birth, Deaths, Marriages and Care which has Child Benefit as one of the services it offers and a replication of this same service in the Department Benefits. The question is this, why can't the Department for benefits make use of the already existing framework the Birth, Deaths, Marriages and Care department has? Is there the need for the user of the system to fill this information independently for each department? The following results analyse the data in the ontology to attempt to answer the queries posed, highlighting the perceived threats and risks emergent from the data. The results have been cut down slightly for the purposes of the paper and are therefore illustrative rather than exhaustive and are an indication of how inferencing could potentially help in the analysis of risks in the E-Government domain:

1. What are the typical objectives of a benefit service?

nRQL Query: (retrieve (?obj) (?obj |Objective|))

nRQL Result: (((?OBJ |Data_Confidentiality|))

((?OBJ |Availability|))

((?OBJ |Data_Integrity|))

((?OBJ |User_Eligibility|))

((?OBJ |User_Accountability|))

((?OBJ |User_Non_Repudiation|))

((?OBJ |Accuracy|)))

In order to answer this question, we first highlight the objectives of the Benefit service. This enabled the modelling of the goals of this service into the ontology.

2. Which assets are confidential in a benefit system?

nRQL (retrieve (?asset) (and Query: (|Confidentiality| ?threat

|is_threatened_by|) (?asset ?threat

|damaged_by|)))

nRQL (((?ASSET |Benefit_Data|))

Result ((?ASSET |Personal_Data|))

((?ASSET |Cryptographic_Keys|)))

In order to address the question of confidentiality in the Benefit service, we had to examine potential threats to the confidentiality of citizens. In doing so we first had to determine the possible threats to the confidentiality of citizens, and model the assets that may be compromised or damaged by them. So, in the case of confidentiality, we modelled that the confidentiality of a citizen may be threatened by, for example user errors, cryptographic keys disclosure or compromise etc.

3. What are the typical objectives of the Births, Deaths and Marriages service?

nRQL Query: (retrieve (?obj) (?obj |Objective|))

nRQL Result: (((?OBJ |Data_Confidentiality|))

((?OBJ |Availability|))

((?OBJ |Data_Integrity|))

((?OBJ |User_Eligibility|))

((?OBJ |User_Accountability|))

((?OBJ |User_Non_Repudiation|))

((?OBJ |Accuracy|)))

In order to answer this question, we first highlight the objectives of the Births, Deaths and Marriages services. This enabled the modelling of the goals of this service into the ontology.

4. Which assets are confidential in the Births, Deaths and Marriages service?

nRQL (retrieve (?asset) (and

Query: (|Confidentiality| ?threat

|is_threatened_by|) (?asset ?threat

|damaged_by|)))

nRQL (((?ASSET |Benefit_Data|))

Result : ((?ASSET |Personal_Data|))

((?ASSET |Cryptographic_Keys|)))

In order to address the question of confidentiality in the Births, Deaths and Marriages service, we had to examine potential threats to the confidentiality of citizens. In doing so we first had to determine the possible threats to the confidentiality of citizens, and model the assets that may be compromised or damaged by them. So, in the case of confidentiality, we modelled that the confidentiality of a citizen may be threatened by, for example user errors, cryptographic keys disclosure or compromise etc. Questions 1-4 show us that the Benefits service and Births, Deaths and Marriages service have the same objectives. Therefore, there is a potential for reuse between these services.

5. What happens to departments that are dependent on other departments for shared resources or information?

nRQL (retrieve (?dependency)

Query: (|Department functionality| ?risk is_threatened_by|))

nRQL (((RISK |Over_Dependence|))

Result: ((?RISK |System_Failure|))

((?RISK |Shared_Points_Of_Failure|))

((?RISK |Security_Compromise|))

((?RISK |Reduced_System_Reliability|))

((?RISK |End_Of_Service|))

((?RISK| Decommissioning _Of_Department|)))

In order to answer this question, a list of potential risks had to be developed and structured for the ontology some of which are highlighted in the example above including Over Dependence, System Failure, Shared Points of failure, Security of the system being compromised, the reliability of the system being reduced and even abolition of a department which could lead to the termination of the service or services offered by that department.

6. Which risks might compromise the functionality of a department?

nRQL (retrieve (?risk)

Query: (|Department functionality| ?risk

is_threatened_by|))

nRQL (((RISK |Over_Dependence|))

Result: ((?RISK |System_Failure|))

((?RISK |Shared_Points_Of_Failure|))

((?RISK |Security_Compromise|))

((?RISK |Reduced_Funding|))

((?RISK |Reputation_Damage|)))

In order to model this question into our ontology, we had to determine the risks that may hamper a department meeting its remit to provide functional services to her citizens, with the example above indicating Over Dependence, Security Compromise.

7. Which threats can compromise the anonymity of the users of the system when services are combined?

nRQL (retrieve (?threat)

Query: (|User_Anonymity| ?threat

is_threatened_by|))

nRQL (((?THREAT |Impersonation|))

Result: ((?THREAT |Malicious_Code|))

((?THREAT |User_Error|))

((?THREAT |OS_Bugs|))

((?THREAT |Application_Bugs|))

((?THREAT |Terminal_Highjack|)))

As services are combined and solutions reused across governments, the anonymity of users may be compromised, and we have highlighted a subset of the threats that a user may face if this is the case.

8. Can countermeasures be put in place so that there is no impersonation in the systems that are combined?

nRQL (retrieve (?citizens information)

Query: (?Citizens Information |No_Impersonation| |address|))

nRQL (((?Citizens Information |Identification|))

Result: ((?Citizens Information |Authentication|))

((?Citizens Information |Audit_Trails|)))

The example above shows that for this example to prevent impersonation in combined systems, audit trails would be beneficial.

9. Can dependencies among services bring about inter-departmental co-operation?

nRQL (retrieve (?dependency)

Query: (|Inter-departmental co-operation| ?dependency|))

nRQL (((? Co-operation |Optimized Results|))

Result: ((?Co-operation |Increased_Communication|))

((?Co-operation |Cognitive_Complexity|))

((?Co-operation |Enhanced_Solutions|)))

Co-operation between departments foster partnerships and collaboration. This involves having joint goals and a reliance on departments to accomplish the goal. When concepts from an ontology are imported from other ontologies, the dependencies that exist among them are managed using the reproduction of concepts to be imported (Kozaki et al. 2007). In the same vein, when dependencies amongst services exist, they reproduce all definitions related to the concepts produced. Services that are delivered in silos take more time in problem resolution. This could involve sending a client to multiple locations and could lead to information that is incomplete or inaccurate.

5. In Conclusion

In this paper, we have discussed the role of ontologies in the delivery of E-Government services, the advantages of reusing the components and solutions that cut across these services as well as the inherent risks and challenges that a government may face with reusing components. The use of ontologies provides an effective means of capturing, describing and exploiting knowledge in the area of E-Government with its rapidly evolving departments and services. We presented the use of a developed E-Government ontology in multiple areas of application in Electronic Government for gauging risks that may face a government in areas of reuse. A major challenge faced in modelling the ontology is the fact that the E-Government domain is an expansive one and insufficient tools have been developed to date during the research to enable accurate curation of all relevant terms. Once further developed and supported by a suitable set of user tools the testing of the ontology in a national setting, currently planned to be that of the Nigerian government will take place.

References

Fonou-dombeu, J.V. & Huisman, M., 2011. Semantic-Driven e-Government : Application of Uschold and King Ontology Building Methodology for Semantic Ontology Models Development. , 2(4), pp.1–20.

Gmbh, R.S., 2010.

RacerPro Reference Manual Version 1.9.

Gruber, T.R., 1993. Toward Principles for the Design of Ontologies Used for Knowledge Sharing. , pp.907–928.

Gugliotta A, Cabral Liliana & Domingue John, 2005. Knowledge modelling for integrating semantic web services in e-government applications Conference Item.

Gugliotta, A. et al., 2005. A conceptual model for semantically-based e-government portals.No Title. In 1st International Conference on eGovernment ICEG. Ottawa, Canada.

Homburg, V., Bekkers, V. & Rotterdam, N., 2002. The Back-Office of E-Government (Managing Information Domains as Political Economies) Center for Public Management The Dutch Setting : Networks of Governmental Organizations and The Political Economy of Information. , 00(c), pp.1–9.

Karyda, M. et al., 2006. An ontology for secure e-government applications.

Kozaki, K. et al., 2007. A Framework for Cooperative Ontology Construction Based on Dependency Management of Modules. , (November), pp.33–44.

Noy, N.F. & McGuinness, D.L., 2001. Ontology Development 101: A Guide to Creating Your First Ontology,

Sheng, L. & Lingling, L., 2011. Application of Ontology in E-Government. 2011 Fifth International Conference on Management of e-Commerce and e-Government, pp.93–96. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6092638 [Accessed April 22, 2014].

Sowa, J.F., 2000. Knowledge representation: logical, philosophical and computational foundations, Pacific Grove, CA, USA: Brooks/Cole Publishing Co.

Stumme, G., Studer, R. & Sure, Y., 2000. Towards an Order-Theoretical Foundation for Maintaining and Merging.

Uschold, M. & Gruninger, M., 1996. Ontologies: Principles Methods and Applications. Knowledge Engineering Review, 11(2), pp.1–63.

Woll, R., Geißler, C. & Hakya, H., 2013. Modular ontology design for semantic data integration. , pp.3–6.

Appendix II: Publication

THE USE OF ONTOLOGIES TO GAUGE RISKS ASSOCIATED WITH THE USE AND REUSE OF E-GOVERNMENT SERVICES

Onyekachi Onwudike	Russell Lock	Iain Phillips
Dept of Computer Science	Dept of Computer Science	Dept of Computer Science
Loughborough University	Loughborough University	Loughborough University
o.c.onwudike@lboro.ac.uk	R.Lock@lboro.ac.uk	I.W.Phillips@lboro.ac.uk

ABSTRACT

E-Government ontologies have been developed for different strata of government over a number of years. However, the majority of these ontologies have had little or no impact on E-Government as a whole. The development of E-Government ontologies in isolation, without wider integration in perspective and the lack of reuse of components present serious challenges for the E-Government domain. Although the idea of reuse across ontologies seems to be a welcome idea with respect to the problem of interoperability, the risks and disadvantages associated with reusing existing solutions, as well as making certain functionalities sharable between E-Government services, is a relatively new area of research.

This reuse of existing solutions may potentially help to foster co-operation amongst E-Government departments, reduce costs and reduce development time as well as increase reliability and maintainability of such systems. This paper explores existing E-Government ontologies and assesses the assistance a suitably designed ontology could have in reducing system development and evolution risks. It incorporates the development of a new ontology for E-Government and explores the role of ontologies in overcoming risks that may be associated with service combinations such as overlapping of services, the uncontrolled reuse of components, monopoly of information across departments and areas of dependency resulting in conflict amongst others. The listed scenarios avail us the opportunity to investigate if some combination of services are beneficial especially in cases where there is service dependence amongst services. We conclude that the use of ontologies could play a significant role in gauging the risks associated with this.

KEYWORDS

E-Government, Risks, Threats, Ontology, Reuse

1. INTRODUCTION

Any large-scale system should be developed to support evolution. Most sustainable systems are subject to on-going change and these changes to a system can take place for a variety of reasons. The reasons behind the development of a system may be invalidated because of changes which may not have been foreseen from the initial development of the system; redundancy of the system; expansion of the system to incorporate new services; changes in user needs and requirements amongst others. One of the major problems in handling knowledge representation practically is the aspect of dealing with relationships that change with the passage of time (Welty & Fikes 2006). This problem is made more complex since most modelling languages are limited in their expressive power considering that they are restricted to binary and unary relations. The complication is also made worse because most representation languages overlook the specification of time.

The concept of E-Government is well-established with numerous service providers offering similar services to citizens, businesses and governments. However, most of these services are composed of service components that are similar. Therefore, the reuse of domain knowledge is significant in this research as this can contribute greatly in the area of effort reduction and quality of service improvement. It is currently difficult to answer questions such as "what difficulties or threats can arise when information is exchanged across departmental boundaries?" or "can dependencies among services result in conflict?" In areas such as business and engineering, metrics are used to determine the health of a project and whether the dividends justify the costs. The threats that face any enterprise are critical to the advancement and growth of that enterprise. Looking at the E-Government domain as an enterprise especially with respect to the delivery of services, there is a possibility of making incorrect or unwise decisions when it comes to the reuse of service components, the threats such reuse and combination of components bring about as well as the possible countermeasures. When services are developed in silos, they are prone to a number of risks including a lack of communication between departments which could potentially introduce shared points of failure thereby reducing the resilience of the system. It is one thing to chant the chorus of reuse; it is quite another to discover the effects these have on the E-Government

domain. Since there is no precise definition of the adverse effects lack of reuse can bring about in the E-Government domain, there is confusion among Service Providers on which services can be combined and which components of these services can be reused. Therefore, an ontology to gauge the risks and threats associated with this is a viable solution to this problem. The reason for this is that the entities in an ontology would be defined in a sound manner and relationships such as dependencies that exist amongst entities would be precisely specified. Furthermore, the use of an ontology would give decision makers greater depth as to why certain decisions should be made when it comes to Electronic services in the E-Government domain. Having seen that decisions are mainly made by managers who have little or no knowledge about the underlying infrastructure on which the E-Government domain is built upon and who base decisions on intuitions rather than on defined metrics, the use of an ontology can be used to greatly reduce this (Singhal 2010).

Therefore, the key goals of this research are to:

1. develop an ontology which can be used to identify threats that endanger the E-Government domain in areas such as:
    - component reuse
    - component combination
    - asset procurement
2. incorporate countermeasures that can be taken to counteract the threats that would be identified or better still reduce the probability of system fatality.

The structure of the remaining paper is as follows section 2 introduces us to E-Governments and their corresponding ontologies; section 3 explores the aspect of component reuse. In section 4, we define constructs for the intended ontology and in section 5, we point out risks that may exist as a result of combining components. Section 6 presents the language for developing the ontology and section 7 concludes the work as well as provides room for future work.

2. E-GOVERNMENT ONTOLOGIES

Electronic Government often known as E-Gov was established in the late 1990s. The reason behind its establishment was to foster relationships between government and the public so that citizens can effectively and efficiently interact with government (Layne & Lee 2001). The onus lies on governments all over the world to implement E-Government in order to

improve the state of governance and delivery of services to her citizens by eliminating processes that are inefficient as well as time-consuming.

In line with the reason for its establishment, it has as its main objective the development of solutions that are technological which can support interactions between citizens and public institutions which would improve public participation, social life as well as serve as a means for reducing cost (Barbagallo et al. 2010). It is worth noting that E-Government is not limited to the publishing of information on the internet or on websites but involves understanding the structure and operations of different departments and administrations. Often governmental demands for improvements to services clash with citizen requirements. An example can be seen in the development of policies that respond to the needs of the individual as well as their circumstances (Holmes 2011). Therefore, for a government to remain relevant to her citizens, an active role in the implementation of E-Government must be taken into consideration (Mundy & Musa 2010). The reason behind the practice of public administration is the placing of citizens at the centre of policymakers' considerations, not just as the target of the decisions being made but also as agents and drivers of these decisions. E-Government provides services that are used regularly by SPs as well as SRs. With the passage of time, there has been an increased complexity of E-Government services. Correspondingly, this requires increased management (Stojanovic et al. 2004). The problem with governments is that they are very complex and because of this complexity, they are subdivided into different departments with each department offering its own kind of service and operating on a separate budget. However, a major problem is that a general approach is hardly ever employed in the development or distribution of these services. For example, there is reuse of similar components across departments such as the Driver's License Department and the department in charge of issuing passports. This has brought about lack of integration amongst these departments, a lot of repetition and the use of the same kind of components across departments. This has led to development taking place across the government in silos. The potential for reuse and savings across these departments exist and the use of an ontology is a viable technique for achieving this and overcoming the problem of silos in government. This is made possible with the use of an ontology to capture the different activities of these departments as well as model the relationships and interdependencies that exist between them.

An ontology is defined as "*an explicit specification of a conceptualization*" (Gruber 1993). Therefore E-Government ontology can be described as an explicit description of the E-Government domain containing a common vocabulary with shared understanding. E-Government is a domain which must be carefully considered because it deals with the use of Information technologies in providing better government to citizens. Concepts and relations managed by any scientific community need to be formally defined and the use of ontologies support their definition. Several E-Government ontologies have been developed such as SmartGov, EGov, OntoGov, TerreGov etc. Most of these ontologies are already obsolete and lack semantic consistency which has led to loss of critical information. However,(Gugliotta A et al. 2005) argue that no one of these ontologies adopt the Semantic Web technologies to represent concepts and actions.

The question may arise, why are the ontologies previously developed not being applied today?

According to (Fonou-dombeu & Huisman 2011), ontologies are used to describe and specify E-Government services (E-services), primarily because semantic integration and interoperability of E-services are facilitated with their use; there is ease in composition, matching, mapping and merging of various E-Government services. In the context of this paper, the domain of an E-Government ontology comprises of issues that are government related. Therefore the purpose of the E-Government ontology is to facilitate adequate understanding of the E-Government domain by service providers so that issues relating to the integration of services as well as the risks associated with integration in the E-Government domain can be addressed as well as used as prediction tools for future governments. It is practically impossible to develop a single ontology that satisfies all users especially in the areas of precision, coverage, actuality and individualization. This can be attributed to the fact that specific approaches as well as vocabularies are needed by different departments for solving tasks specific to them (Stumme et al. 2000).

Ontologies serve as a platform or a means for defining the services offered by governments and attempts have been made at the development of E-Government ontologies. The use of ontologies for knowledge representation enhances organization, communication and re-usability as well as serve as the building blocks for intelligent systems. This has been of immense benefits as seen in applications.

3. LITERATURE REVIEW ON COMPONENT REUSE

For a government to meet her objectives in a cost-effective and timely manner, applications should be made reusable by other software. It is also possible for a solution developed by one government to be reused by another government (Ratneshwer & Tripathi 2010). This can be seen in some EU system developments such as the ECRIS system which is designed to provide international access to criminal records.

Globally, across most industries, about 85% of the processes that take place across various departments are the same. This is applicable also to the processes that take place across government organizations (Anon 2003). It is therefore logical to cultivate the reuse of software where possible as the reuse of solutions may potentially help to foster co-operation amongst departments, reduce costs, reduce development time as well as increase reliability and maintainability of such systems.

Most software are developed in component or modular form and the act of developing these reusable components is known as Component-Based Development. The Netherlands is a country that ensures collaboration between departments as well as makes use of component-based development. Collaboration amongst departments is even seen between small municipalities in the Netherlands. This is aimed at elimination of duplicated efforts and to establish one shared back-office (Janssen & Wagenaar 2004). Since services cannot always be provided at reduced costs and implemented locally; organizations that are small and limited by budgets and expertise cannot develop all the services that are desired, by sharing services and expertise among organizations, a larger number of services can become widely available. (Sheng & Lingling 2011) identified information and data sharing as the cornerstone for E-Government. In the process of integrating data we discover that beyond information sharing, resources can also be shared which we believe can bridge gaps as well as foster trust in the E-Government domain. Considering that there are varying degrees of information, data and component reuse across departments and even governments, there are also risks and disadvantages associated with reuse which would be identified in the questions this research would attempt to answer. Although component reuse across departments is essential in the sense that they are built with common functionalities and attributes and therefore can be deployed into a new system with modifications to suit the requirements of the system; they pose inherent challenges.

This may help to greatly reduce development time and costs. This would greatly increase the reliability and maintainability of the system (Ratneshwer & Tripathi 2010). But the question arises although the goal of E-Government should be the delivery of services to her citizenry, is there a way that the people behind the delivery of these services can work jointly? In the area of a joint work force, as stated by (Homburg et al. 2002) there is often a requirement of information exchange in the back offices of government. It is usually difficult to establish a joint workforce because most of the ontologies are developed in isolation and sometimes with no possibility of reuse in mind. The need for collaborative development is key because the influence of modification of ontologies can be effectively managed (Sunagawa et al. 2003). Although (Sunagawa et al. 2003) established the need for collaborative development across E-Government ontologies, can we say this was adhered to? (Vasista 2011) in his paper also viewed this collaborative problem as "*the inability of existing integration strategies to organise and apply the available knowledge to the range of real scientific, business and governance issues"*. This he believed to impact not only on the productivity of a government but also the level of transparency of information in crucial safety and regulatory applications. He however proposed focussing on models of E-Government that are normative which can assert integration of data both horizontally and vertically. This form of assertion is supposed to be reusable by several E-Government applications.

4. DEFINITION OF A SERVICE CONSTRUCT FOR THE ONTOLOGY

In defining a service construct for this ontology, the need to focus on these areas are key because the definition of a service with respect to this ontology requires a construct that is generic enough to allow the specification of any kind of service.

a) **Cataloguing**: Cataloguing is an important aspect of E-services. This aspect of a service should enable users locate services without having to go through tedious processes. This entails categorizing services in form of informational services which would aid the easy location of compatible options for sub-services.
b) **Combination of services**: Services which have constructs that are similar can be combined because this would fully aid servicing the needs of a customer or citizen. Exploring services that are composed of sub services also entails mapping of services with similar constructs or mapping similar services to an integrated or generic service.

c) **Change management**: Incorporating the changes that occur in the system is another very interesting aspect of this ontology. By change management, proper documentation of changes such as releases, updates, failures in the system, date of commissioning and decommissioning of the system or parts of the system are taken into account. This we find an essential bit of the ontology that should be incorporated. Changes take place all the time and a mechanism for updating the areas undergoing change must be in place. This aspect of change management greatly informs of the inherent dangers certain combinations of services or subservices could cause.

Table I presents one of the key building blocks of our ontology in development showing the semantic relationship necessary to specify that a person belongs to a department and a department offers a service. A service can further be divided into sub-services which can be made up of similar components. Table II explains what a leaf service is which means that a service can stand on its own without being composed of sub-services. Table III presents the axioms that are important in the development of this ontology.

Table I: Defining the Ontology Construct

Definition	**Description**
Person (p)	*p* is a person and belongs to *d*
Department *(d)*	*d* is a department
p → d	Person offers service and is a member of department
offers service *(s, ss)*	Where service s has a sub service *ss*
has components (c)	service (s,ss) is made up of components (c)

Table II: Defining the service construct

Definition	**Description**
Service *(s)*	*s* is a service
Has subservice *(s, ss)*	Service s has a sub service *ss*
Leaf service (ls) → ((∀*s)(¬ has subservice(ss, s)))*	A leaf service is a service that has no subservice

Table III: Defining axioms for the service construct

Axiom 1. If *sb* is a subservice of *sa*, and *sc* is a subservice of *sb*, then *sc* is a
subservice of *sa*.
has_subservice(sa, sb) ∧ has_subservice(sb, sc) →has_subservice(sa, sc)
Axiom 2. No service is a sub-service of itself
¬has_subservice(s, s)
Axiom 3. If *s2* is a subservice of *s1*, then *s1* cannot be a subservice of s*2*.
has_subsevice(s1, s2) → ¬ has_subservice(s2, s1)

In an attempt to reuse bits of E-Government ontologies, different ontologies (SmartGov, OntoGov, TerreGov, EGov) have been written by different authors for different purposes, with different assumptions, and with the use of different vocabularies. Also, in testing and diagnosing individual or multiple ontologies, the discovery that different authors were using relational arguments in differing orders and thus type constraints were being violated across ontologies was evident. Additionally, if a relation's domain and range constraints were used to conclude additional class membership assertions for arguments of the relation, then those arguments could end up with multiple class memberships that were incorrect.

Ontologies may require small, yet pervasive changes in order to allow them to be reused for slightly different purposes. Increasingly e-government services are being developed that cut across old department lines and there is an increasing need for intra and inter-governmental agencies to work more closely together, moving towards joined- up government. With this change comes the need for better communication between people and a need for a common vocabulary and understanding of terms that are being shared.

5. DESIGNING AN ONTOLOGY TO GAUGE RISKS AND THREATS ASSOCIATED WITH E- GOVERNMENT

Having an understanding of the kind of threats that may take place when services are combined gives us an insight into the conflicts and co-operation that may take place at the back office especially with respect to sharing of resources and information property rights.

(Homburg et al. 2002) analysed the effects of resource dependence theory and information property rights theory stating the conflicts that could stem from such mixtures in the network.

The development of modern products requires heavy reliance on the use of IT systems. (Woll et al. 2013) outlined a major challenge associated with this as lack of interoperability between different IT systems. Although a lot of research and industrial activities have focused on the feasibility of interoperability in the past, the problem still lingers.

In editing ontologies, attention should be paid to the influence this has on other ontologies. According to (Sunagawa et al. 2003), changes in an ontology have the potential of eliminating the consistency that exists between the ontologies.

(Woll et al. 2013) also outlined how approaches have been mapped out on embracing interoperability but there is a lack of application in the industry. This they attributed to the high cost of linking many different IT systems and the data contained in them.

To successfully build a platform for E-Government to operate requires the collation of information from the different departments and parastatals that make up the government. Hence, there is a lot of replicated data as data collated for one department may be the same data collated across other departments even though the modes of collation or delivery may differ. A typical scenario seen while building this ontology from the UK Government website is in the department of Birth, Deaths, Marriages and Care which has Child Benefit as one of the services it offers and a replication of this same service in the Department Benefits. The question is this, why can't the Department for benefits make use of the already existing framework the Birth, Deaths, Marriages and Care department has? Is there the need for the user of the system to fill this information independently for each department? Analysis of this scenario based on perceived risks and threats include:

1. Could reuse of components or data affect data resourcefulness?
2. Can dependencies amongst services result in conflict?
3. Can the above scenario bring about shifts in power?
4. What difficulties can arise when information is exchanged across departmental boundaries?
5. Does information or resource sharing bring about conflicts amongst departments?
6. What happens to departments that are dependent on other departments for shared resources or information?
7. What threats, risks and conflicts do these pose to such departments? For example, unforeseen dependencies which embody potential single points of failure
8. Can dependencies among services bring about inter departmental co-operation?

(Potential advantage): When concepts from an ontology are imported from other ontologies, the dependencies that exist among them are managed using the reproduction of concepts to be imported (Kozaki et al. 2007). In the same vein, when dependencies amongst services exist, they reproduce all definitions related to the concepts produced. From figure 1, assuming that ontology B imports concept A3 defined in Ontology A, then we can say that all the concepts depended by A2 are reproduced with relations among them, and Ontology B imports these reproductions. It means all definitions related to the concept are reproduced.

The system reproduces all definitions related to the concept. In this example, “the super concept of A5” (A4 and A1), “the concept referred by A5” (A4).

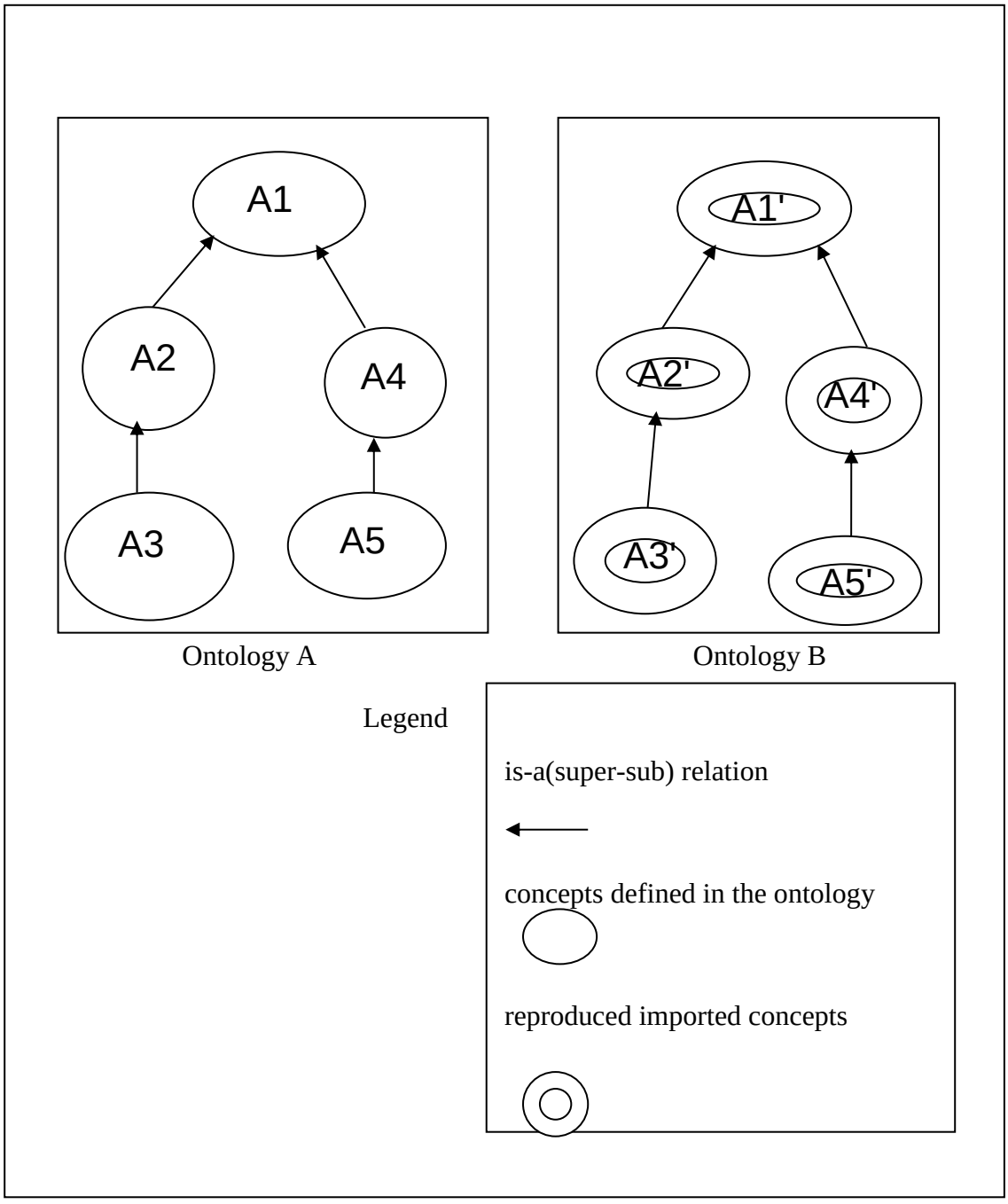


Figure I: Diagram showing dependencies

Figure I: Diagram showing dependencies

6. OWL

The choice of OWL to model our ontology gives us the ability to easily build systems that are interoperable which would enable the production, reasoning and visualization of data in the E-Government domain (OWL 2004). Considering that the E-Government domain is a large one and the amount of data associated with it is quite large and complex; there is need to make use of reasoning components that are highly optimized which is made available through the use of off-the-shelf editors i.e. Protégé (Protege 2005). The main goal of this research is to provide an ontology to support service providers and decision makers in the E-Government domain. The ontology would be able to highlight potential threats and risks which endanger service combinations, component reuse as well as asset procurement and what countermeasures can be taken to lower the chances of attacks and severity.

Since most organizations do not develop products that are entirely new at every stage of development, there is an increasing demand for the reuse of existing products and models. The reuse of products or models is one that suffers from lack of interoperability especially in the area of missing tools. (Woll et al. 2013) stated that challenges with reusing models lies in choosing the right one to make use of; adding that the development of a suitable model to reuse is largely dependent on the requirements and functions of the new product. Considering the knowledge, experience and expectations service providers have about E-Government ontologies, there should be a means by which the performance of these E-Government ontologies are evaluated. One of the goals we have in the area of developing the ontology in terms of reusable components is to make certain functionalities sharable as well as evaluate the information obtained to make certain decisions. The question is, by what standards would we be able to evaluate this ontology? We want to believe that in terms of this research, service providers across government share a common understanding of what a service means to a SR. This serves as a platform to design the needs of the receiver. We also use this as a yardstick to determine what kind of detail a service provider may be interested in as well as the amount of detail the proposed ontology should contain. A major area identified is in the area of information exchange and dependence in the networks of back offices. This avails us the opportunity to analyze areas of conflict and cooperation that arise from the complex mixture of the services provided. Based on this line of thought, a reasoning engine or tool would be incorporated against the ontology that produces a list of departments

offering a particular service as well as make inferences on whether certain service combinations are needed and what risks they pose. This would be achieved with the use of semantic technologies to achieve interoperability and integration between the E-Government systems. This can serve as a support tool for the stakeholders of the system (government, service providers, software developers) responsible for systems which are in use. With the definition of a viable tool which can be used to solve problems faced in the E-Government domain; this tool should be able to store data obtained from the ontologies as well as computationally solve the problems listed in the above scenarios.

6.1 REPRESENTATION OF ROLES IN THE ONTOLOGY USING OWL

Understanding the meaning of Role in the development of an ontology is very important. Although the usefulness of OWL in ontology representation cannot be under-estimated, semantic interoperability can equally be decreased because of gaps that may exist between developers and OWL in properly defining roles (Kozaki et al. 2007). Therefore, in order to overcome this problem, a clear understanding of the roles of a Service Provider in the E-Government domain are needed. Within our ontology, a key concept is the concept of Service Provider. We analyze the activities of a Service Provider and the roles he plays in the examples below. Service Provider joins the E-Government domain to publish his service. However, he has to choose an appropriate department to which his service maps. It is also possible for a Service Provider to map to different departments offering different services. If a ServiceProvider chooses to map a service to a non-existent department within the ontology, the ontology allows him to create a new department to map his services to. Therefore, the ServiceProvider can readily associate with an existing department in the ontology or he can update the ontology with a new department and associate with the new department. Our model distinguishes between two principle types of role, those of service provider, and service reciever. A ServiceProvider is a person able to carry out several different roles. Therefore, it is worth noting that his role would potentially involve a one-to-many-relationship.

Figure II shows three examples of our role representation model for the ServiceProvider in the ontology being developed. Each of these examples is evaluated according to the requirements for dealing with roles. With respect to our ontology, the ServiceProvider Role is dependent on a department as its domain. Comparison among Figures IIa, b and c show three examples of our role representation model in OWL.

Example 1 (in Figure IIa): the role of a ServiceProvider is dealt with in serviceProviderOf property. This object property may represent the role which is determined in e.g. "ServiceProvider-ServiceReceiver relation". However, the context dependency of the concept of roles is implicit. A critical problem therefore arises because the context dependency relates to other characteristics essentially.

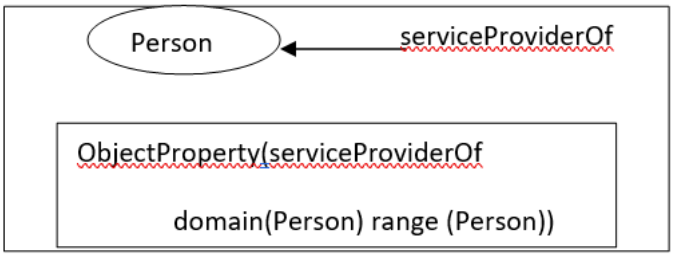


Figure IIa: Role Representation model 1

Example 2 (in Figure IIb): This model represents the context of ServiceProvider explicitly. This role is still dealt with in a property. This can complicate management of identity of roles in its instance model. For example, it is difficult to describe that after a particular ServiceProvider resigns from his role as a ServiceProvider, another person can easily fill this role as the ServiceProvider. This model is not intended to represent state of the role concept. This means that a vacant role would be difficult to represent or identify.

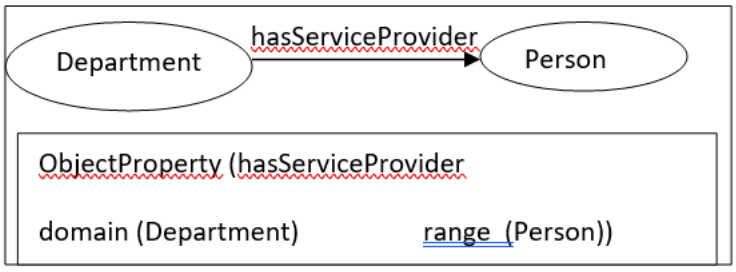


Figure IIb: Role Representation model 2

Example 3 (in Figure IIc): The hasPart property in this model of our ontology means that a Department consists of Service Provider(s). Therefore, a restriction placed on dependOn property in ServiceProvider class shows that a ServiceProvider depends on Department as its domain in this context. This model is superior to the above two models because their problems can be solved in this model. However, a ServiceProvider is classified into a Person which can also be confused with the concept of role; ServiceProvider. According to

the semantics of rdfs:subClassOf, an instance of a ServiceProvider and its player (an instance of Person) are required to be one and the same instance. The player can therefore not stop to be an instance of a ServiceProvider without stopping to be an instance of a Person, i.e., deletion of an instance of a ServiceProvider brings with it the deletion of an instance of a Person.

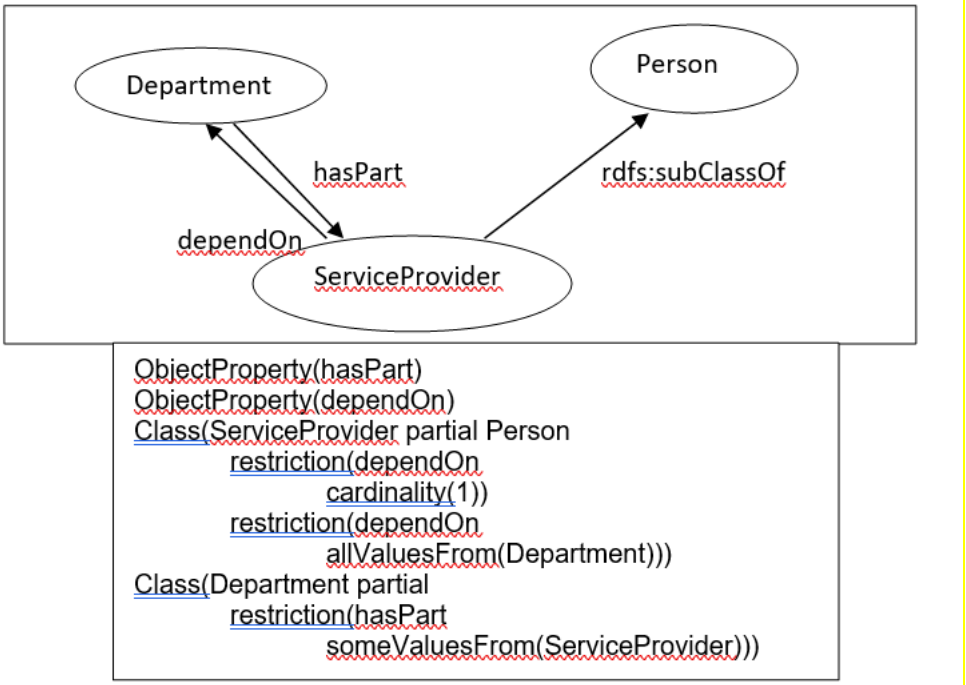


Figure IIc:Role Representation model 3

7. CONCLUSIONS AND FUTURE WORK

In this paper, we have discussed the role of ontologies in the delivery of E-Government services, the advantages of reusing the components that cut across these services as well as the inherent risks and challenges that a government may face with reusing components. We present the role a suitably designed OWL ontology could play in the delivery, management and evolution of E-Government services. The model presented in this paper predominantly focuses on the specification of a general service construct which represents the various roles and characteristics of a service. The ontology under development contributes to the semantic interoperability that should exist in E-Government ontologies and also provides a novel potential approach to solving the problems caused by reuse of components.

In terms of future work, we plan to investigate the key problems caused by reuse of services and service components as well as enhancing and investigating the resilience of our tool on an existing real-world government case study.

REFERENCES

Anon, 2003. The Greenhouse Effect. Available at: http://www.academon.com/essay/the-greenhouse-effect-18937/ [Accessed August 11, 2014].

Barbagallo, A., De Nicola, A. & Missikoff, M., 2010. eGovernment Ontologies: Social Participation in Building and Evolution. *2010 43rd Hawaii International Conference on System Sciences*, pp.1–10. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5428280.

Fonou-dombeu, J.V. & Huisman, M., 2011. Semantic-Driven e-Government : Application of Uschold and King Ontology Building Methodology for Semantic Ontology Models Development. , 2(4), pp.1–20.

Gruber, T.R., 1993. Toward Principles for the Design of Ontologies Used for Knowledge Sharing. , pp.907–928.

Gugliotta A, Cabral Liliana & Domingue John, 2005. Knowledge modelling for integrating semantic web ser- vices in e-government applications Conference Item.

Holmes, B., 2011. Citizens ' engagement in policymaking and the design of public services. , (1).

Homburg, V., Bekkers, V. & Rotterdam, N., 2002. The Back-Office of E-Government (Managing Information Domains as Political Economies) Center for Public Management The Dutch Setting : Networks of Governmental Organizations and The Political Economy of Information. , 00(c), pp.1–9.

Janssen, M. & Wagenaar, R., 2004. Developing Generic Shared Services for e- Government. *Electronic Journal of E-Government*, 2(1), pp.31–38.

Kozaki, K. et al., 2007. Role Representation Model Using OWL and SWRL.

Layne, K. & Lee, J., 2001. Developing fully functional E-government: A four stage model. *Government Information Quarterly*, 18(2), pp.122–136. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0740624X01000661.

Mundy, D. & Musa, B., 2010. Towards a Framework for eGovernment Development in Nigeria Independent Researcher , UK. , 8(2), pp.148–161.

OWL, 2004. OWL Web Ontology Language Overview. Available at: Web Ontology Language (OWL),.

Protege, 2005. The protégé ontology editor and knowledge acquisition system. Available at: http://protege.stanford.edu/.

Ratneshwer & Tripathi, A.K., 2010. SOME COMPONENT GENERATION APPROACHES FOR E-GOVERNANCE SYSTEMS. *International Journal of Public Information Systems*, 2, pp.133–147.

Sheng, L. & Lingling, L., 2011. Application of Ontology in E-Government. *2011 Fifth International Conference on Management of e-Commerce and e-Government*, pp.93–96. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6092638 [Accessed April 22, 2014].

Singhal, A., 2010. Ontologies for Modeling Enterprise Level Security Metrics Categories and Subject Descriptors. , pp.5–7.

Stojanovic, L. et al., 2004. On Managing Changes in the ontology-based E- Government. In *On the Move to Meaningful Internet Systems*. pp. 1080–1097.

Stumme, G., Studer, R. & Sure, Y., 2000. Towards an Order-Theoretical Foundation for Maintaining and Merging.

Sunagawa, E. et al., 2003. Management of dependency between two or more ontologies in an environment for distributed development.

Vasista, T.G.K., 2011. S EMANTIC D ATA I NTEGRATION A PPROACHES. , 2(1).

Welty, C. & Fikes, R., 2006. A Reusable Ontology for Fluents in OWL. In *Proceedings of the 2006 conference on Formal Ontology in Information Systems*. pp. 226–236.

Woll, R., Geißler, C. & Hakya, H., 2013. Modular ontology design for semantic data integration. , pp.3–6.

Appendix III: Examples of IT Services based on Categories

Table A: Types of IT services based on core services

No	Service Type	Service Description
1.	Enterprise Directory Service	Enterprise Directory Services provides a centralized authoritative repository of information about network-based resources (such as computers, printers, applications, and file shares). Thus, it reduces the operating and infrastructure costs of agencies by utilizing a common and standardized secure directory.
2.	Managed Desktop Service	provides consistent, reliable desktop computing services using standardized hardware and software components from major vendors.
3.	Identity and Access Management Service	provides a unified platform for e-business authentication and authorization. Keeps track of who can access a system.
4.	Unified Services	unifies single services into composite ones
5.	Multifactor Authentication Service	combines two or more methods of authentication from independent categories of credentials to verify the user's identity for a login or other transactions.

Table B provides a generic list of IT service examples based on enabling/supporting services. More examples of this are provided in Appendix 1.

Table B: IT Services based on supporting/enabling services

No	Service Type	Description
1.	Active Directory Service	Active Directory is a supporting service that provides workstation authentication/single sign-on, service

		integration for authentication, and configuration management for Windows workstations and Servers
2.	Central Authentication Service (CAS)	Central Authentication Service (CAS) is an authentication mechanism as well as an enterprise single sign-on server for web applications.
3.	Desktop Services	Services that provide assistance with personal and departmental computing needs.
4.	Key Management Service	The Microsoft Key Management Service provides product key information to Microsoft products using the MCCA agreements. The service uses a product key to verify the legitimacy of any Microsoft software before activating it.
5.	LDAP (Lightweight Directory Access Protocol)	Centralized directory service that serves as the basis for existing and upcoming identity management services.

Table C presents examples of IT services which have been compiled from different sources of literature based on different service categories.

Table C: IT services based on service category

No	**IT Service Category**	**IT Service**	**Description of IT Service**
1.	Accounts, Security	Access Management	Manages user access to central IT systems;
2.	Accounts, Communication	Email Service	Provides a complete communication package, including email, integrated instant messaging, online document sharing, calendaring, Web publishing tools, and more
3.	Accounts, Communication	Address Management System (AMS)	allows for the self-service management of email aliases and available accounts.

4.	Software, Help	Managed Desktop Services Tools	Microsoft System Centre Configuration Manager (SCCM) and Windows Update Service (WSUS) provide centralized management to insure download/installation of Windows updates and facilitate standardization of users' desktops and laptops to aid in support.
5.	Security	Identity Verification	Identity verification allows the assurance of a person's identity before granting access to secure applications or a protected system
6.	Accounts, Security	Identity Token	This is used for identifying a user to various systems requiring two-factor authentication. Tokens are provided to any government department affiliate who needs one to access networks or servers protecting sensitive data, or other systems that require two-factor authentication.
7.	Hosting/Security	Crash Plan (Desktop Backup Service	This service backs up devices on the cloud

Appendix IV: Stages of E-Government Models in Relation to Evolution

Based on existent E-Government models, there is a triumph of the digital age with the use of technology. This is seen in the different stages of previously developed models whose emphasis is on the development of E-Government using technology. Some of these models include: Layne and Lee model Layne & Lee (2001)**,** Baum and Di Maios model Baum & Andrea Di Maio (2000)**,** ANAO model (Persson & Goldkuhl 2005; Australian National Audit Office 2000), SAFAD model (Persson & Goldkuhl 2005), Hiller & Bélanger model (Hiller & Bélanger 2001), Moon five stage model (Moon 2002), Keng Siau and Yuan Long's synthesizing e-government stage model (Keng Siau & Yuan Long 2005), Gartners four stage model (Baum & Andrea Di Maio 2000), UN's five stage model (United Nations and American Society for Public Administration 2001).

The stages common to these models are:

i. Information publishing stage: this is a case where information about the services of a governments department are provided using a website.
ii. Interaction Stage: this is the case where an interactive website exists and allows for communication between government and citizens
iii. Transaction stage: at this stage, a website allows business operations to be conducted online
iv. Information sharing stage/ Integration stage: a website which allowed for a change in the relationships between citizens and government and even between government agencies. This integration could be in terms of vertical or horizontal integration
v. Clustering of common services stage: This is the enhancement of collaboration and reduction in intermediaries (between operational processes) to provide a unified and seamless service.

Appendix V: Use Case Scenarios

Figure A presents the use case involving a Third-Party SPs with a focus on third SPs responsible for verifying identities. This use case involves three actors: SR, SP (Internal) and SP (External) and ten use cases describing that a service has to be requested for, forwarded to the appropriate Third-Party SP and then fulfilled. Some of the cases describe conditions that must be verified before a service is fulfilled such as: record checks, service configuration. The Third-Party SP is very important considering that in the UK Third-Party SPs like UK Verify are used by approximately 18 EGov Services to verify identities of SRs. The TRAO framework supports this scenario considering that risks associated with third-party SPs are considered.

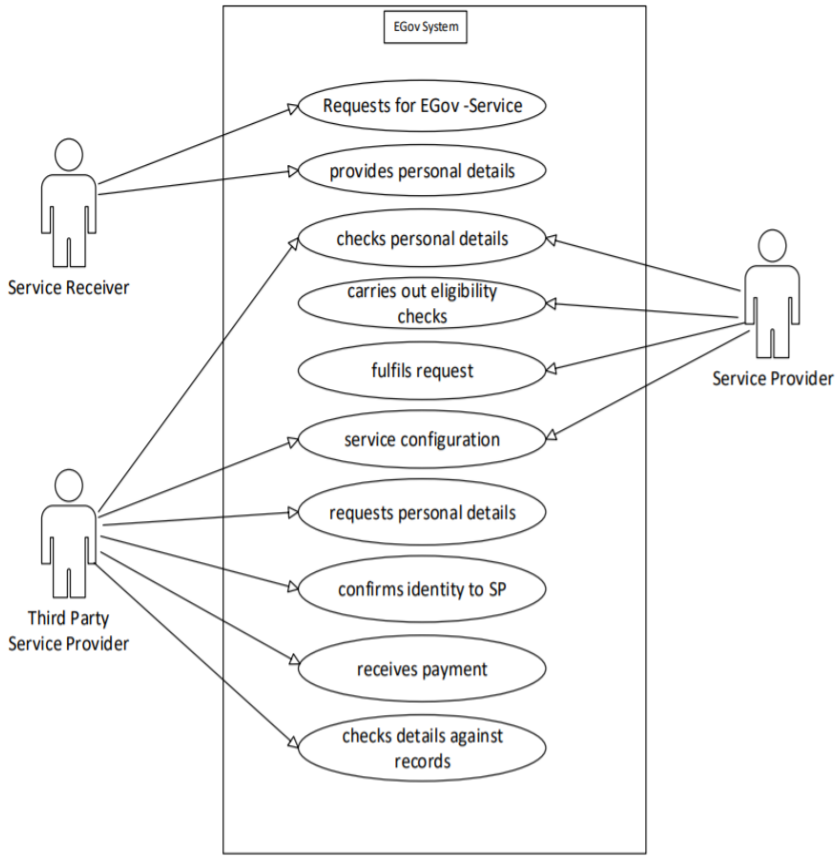


Figure A: E-Gov Third-Party Service Request use Case

Figure B presents a workflow diagram for Third-Party service request. SR initiates a request for a particular service involving the operations of a Third-Party SP. This scenario involves the Third-Party SP asking for personal details, checking those details against existent records, verifying eligibility and if checks are verified positively, then a service configuration is established between the internal SP and the Third-Party SP. Once this happens, the identity of the SR is confirmed to the internal SP and the EGov Service is provided. However, if the checks fail, the EGov Service is denied and the process ends.

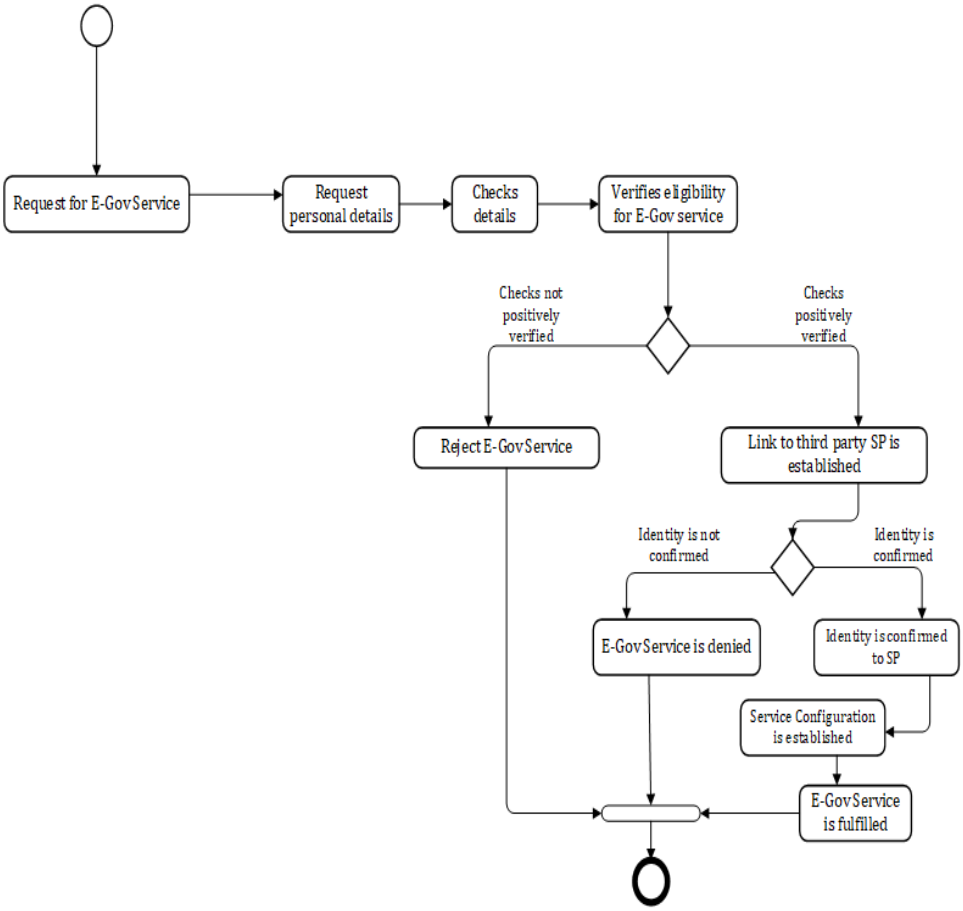


Figure B: Workflow diagram for Third-Party Service Request

Appendix VI: Ontology Modelling

Figure C shows an overview of the logical modelling of the Threat Class

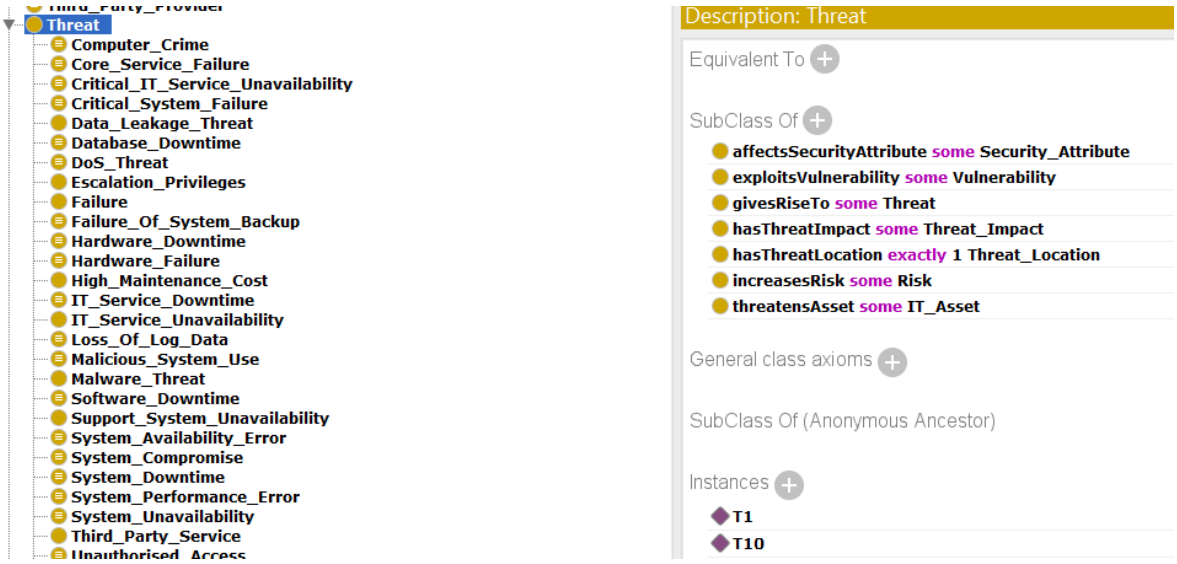


Figure C: Logical Modelling of Threat Class

Figure D shows an example of a threat and the representation of the relationships in its modelling based on the risk it increases and the vulnerability that it exploits

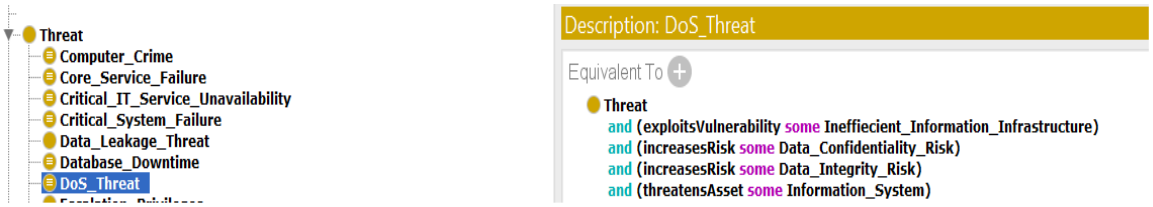


Figure D: Logical Modelling of DOS Threat Example

Figure E shows an example of the Event Class in the ontology

Figure E: Logical Modelling of the Event Class

Figure F presents a logical modelling of the Business Event Class which is also applicable to the other subclasses of the Event Class.

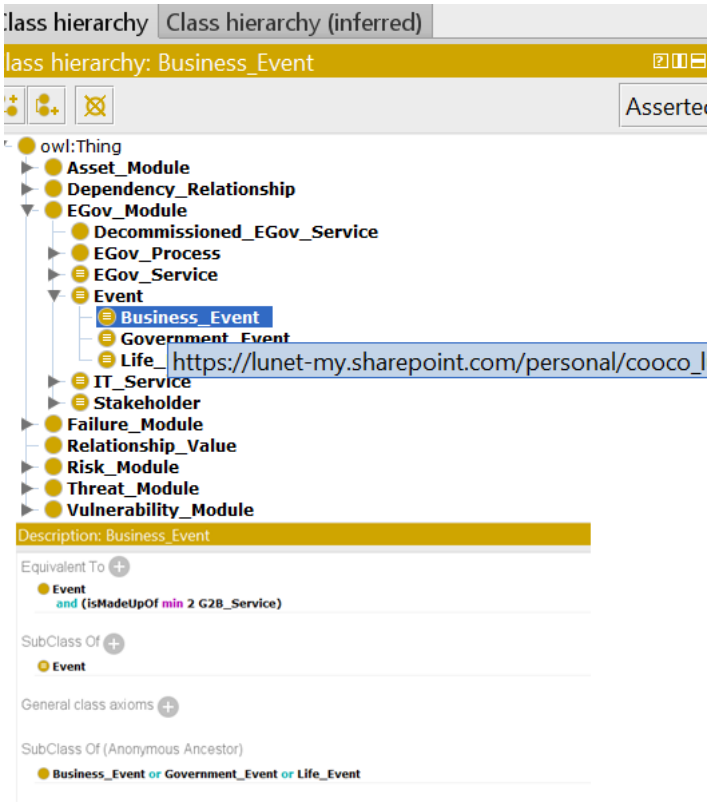
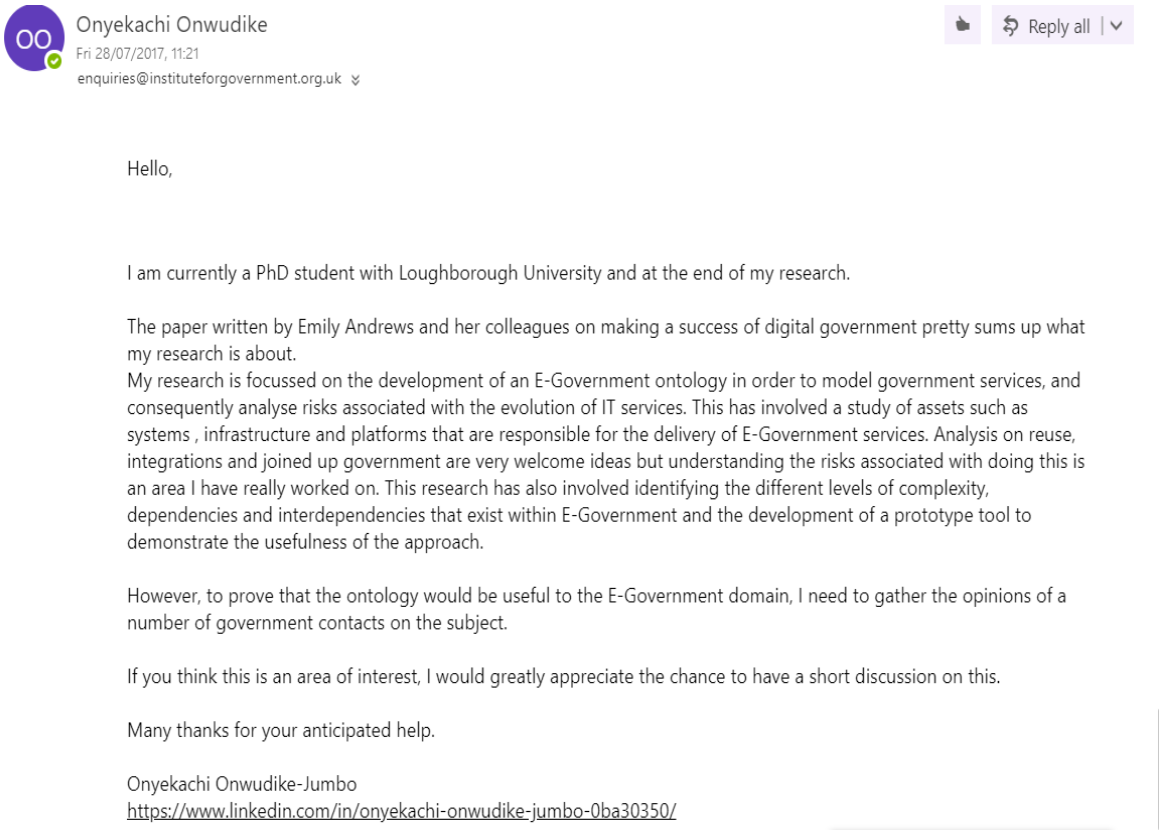


Figure E: Logical Modelling of the Business Event Class

Appendix VII: Evaluation Invitation Email



Onyekachi Onwudike
Fri 28/07/2017, 11:21
enquiries@instituteforgovernment.org.uk

Reply all

Hello,

I am currently a PhD student with Loughborough University and at the end of my research.

The paper written by Emily Andrews and her colleagues on making a success of digital government pretty sums up what my research is about.
My research is focussed on the development of an E-Government ontology in order to model government services, and consequently analyse risks associated with the evolution of IT services. This has involved a study of assets such as systems , infrastructure and platforms that are responsible for the delivery of E-Government services. Analysis on reuse, integrations and joined up government are very welcome ideas but understanding the risks associated with doing this is an area I have really worked on. This research has also involved identifying the different levels of complexity, dependencies and interdependencies that exist within E-Government and the development of a prototype tool to demonstrate the usefulness of the approach.

However, to prove that the ontology would be useful to the E-Government domain, I need to gather the opinions of a number of government contacts on the subject.

If you think this is an area of interest, I would greatly appreciate the chance to have a short discussion on this.

Many thanks for your anticipated help.

Onyekachi Onwudike-Jumbo
https://www.linkedin.com/in/onyekachi-onwudike-jumbo-0ba30350/

Evaluation Questions

Additional questions used during the evaluation include the following

S/No	Question
1	What stakeholders are involved in the Health Service?
2.	What asset components make up the National Infrastructure System and what risks are they exposed to?
3.	what assets are involved in delivering the health service?
4.	What assets degrade after a risk?
5.	Who are the asset owners and Service providers in government?
6.	What are the risks that dependent services face?
7.	What are the vulnerabilities of dependent and supporting assets?
8.	Identify the risks associated with backup assets?