HAROKOPIO UNIVERSITY

SCHOOL OF DIGITAL TECHNOLOGY
DEPARTMENT OF INFORMATICS AND TELEMATICS

Ontology Based Framework for E-Government Regulatory Requirements Compliance

PhD Thesis

Mohammad Mahmudul Hasan

Athens, 2021

HAROKOPIO UNIVERSITY

SCHOOL OF DIGITAL TECHNOLOGY

DEPARTMENT OF INFORMATICS AND TELEMATICS

Οντολογικό Πλαίσιο Συμμόρφωσης Συστημάτων Ηλεκτρονικής Διακυβέρνησης στις Κανονιστικές Απαιτήσεις

Διδακτορική Διατριβή

Mohammad Mahmudul Hasan

Athens, 2021

HAROKOPIO UNIVERSITY

SCHOOL OF DIGITAL TECHNOLOGY
DEPARTMENT OF INFORMATICS AND TELEMATICS

Examining Committee

Dimosthenis Anagnostopoulos (Supervisor)
Professor, Department of Informatics and Telematics
Harokopio University, Athens, Greece

Mara Nikolaidou (Examiner)
Professor, Department of Informatics and Telematics
Harokopio University, Athens, Greece

George Kousiouris (Examiner)
Assistant Professor, Department of Informatics and Telematics
Harokopio University, Athens, Greece

Teta Stamati (Examiner)
Assistant Professor, Department of Informatics and Telematics
Harokopio University, Athens, Greece

Cleopatra Bardaki (Examiner)
Assistant Professor, Department of Informatics and Telematics
Harokopio University, Athens, Greece

Pericles Loucopoulos (Examiner)
Professor Emeritus University of Manchester
United Kingdom (UK)

Panagiotis Kourouthanassis (Examiner)
Associate Professor, Department of Informatics,
Ionian University, Greece

The acceptance of the PhD Thesis from the Department of Informatics and Telematics of Harokopio University does not imply the acceptance of the author's point of view.

Ethics and Copyright Statement

I, Mohammad Mahmudul Hasan hereby declare that:

1) I am the owner of the intellectual rights of this original work and to the best of my knowledge, my work does not insult persons, nor does it offend the intellectual rights of third parties.

2) I accept that Library and Information Centre of Harokopio University may, without changing the content of my work, make it available in electronic form through its Digital Library, copy it in any medium and / or any format and hold more than one copy for maintenance and safety purposes.

Acknowledgements

I owe the heartiest gratitude to my Ph.D. supervisor professor Dimosthenis Anagnostopoulos for his invaluable guidance and support and continuing interest in my field of research work. He has always been involved in my research endeavor, always been critical in improving the quality of the research, always believed in me and, above all always been a mentor. I am also very much thankful to my Ph.D. co-supervisors Professor Pericles Loucopoulos and Professor Mara Nikolaidou for their never-ending encouragement, their guidance is always caring, inspiring, and very generous. I would like to take the opportunity to thank from the bottom of my heart to my co-authors Professors George Kousiouris and Teta Stamati who have given me invariable support throughout the shaping and writing research articles and the Ph.D. dissertation report.

Table of Contents

LIst OF FIGURES

LIST OF TABLES

Abstract in Greek

Η ηλεκτρονική διακυβέρνηση κερδίζει την προσοχή του ερευνητή και του επαγγελματία για την ψηφιοποίηση του δημόσιου τομέα μέσω της θέσπισης πολλών πολιτικών και κανονισμών. Ωστόσο, τα έργα ανάπτυξης συστημάτων ηλεκτρονικής διακυβέρνησης συχνά αντιμετωπίζουν αβεβαιότητες και προβλήματα λόγω γκρίζων περιοχών στους κανονισμούς ή περιορίζονται από υφιστάμενους κανονισμούς για την υιοθέτηση νέων τεχνολογιών και λύσεων στις υπηρεσίες ηλεκτρονικής διακυβέρνησης. Επιπλέον, νέοι κανονισμοί αναπτύσσονται στη δημόσια διοίκηση για την υποστήριξη της αναδυόμενης ψηφιακής διακυβέρνησης. Ως εκ τούτου, η συμμόρφωση με τις κανονιστικές απαιτήσεις που προκύπτουν από αυτές τις πολιτικές και κανονισμούς είναι υποχρεωτική κατά την ανάπτυξη του συστήματος ηλεκτρονικής διακυβέρνησης. Η ανεπαρκής κατανόηση αυτών των κανονισμών στην ανάπτυξη του συστήματος ηλεκτρονικής διακυβέρνησης συχνά οδηγεί σε μερική και, σε ορισμένες περιπτώσεις, ολική αποτυχία του έργου. Επομένως, τα έργα ανάπτυξης συστημάτων ηλεκτρονικής διακυβέρνησης έχουν την ανάγκη για υψηλή συμμόρφωση με τα υπάρχοντα και / ή τα επερχόμενα ρυθμιστικά πλαίσια. Ωστόσο, ο τρόπος με τον οποίο μια νομοθεσία μπορεί να επηρεάζει τα έργα ανάπτυξης του πληροφοριακού συστήματος ηλεκτρονικής διακυβέρνησης συχνά δεν είναι εύκολα αναγνωρίσιμος λόγω της έλλειψης σαφούς κατανόησης των κανονιστικών απαιτήσεων καθώς και του χάσματος μεταξύ των νομικών επιστημών, της ηλεκτρονικής διακυβέρνησης και της Τεχνολογίας της Πληροφορίας. Επιπλέον, λόγω της συχνής ενημέρωσης του νομοθετικού περιεχομένου, είτε σε τοπικό, περιφερειακό είτε σε ευρύτερο επίπεδο (π.χ. σε επίπεδο ΕΕ), αυτές οι πτυχές πρέπει να προσδιοριστούν σαφώς και τα αποτελέσματά τους να γίνουν κατανοητά σε διάφορα επίπεδα ανάπτυξης του συστήματος πληροφοριών ηλεκτρονικής διακυβέρνησης.

Αυτή η μελέτη αρχικά παρουσιάζει ένα οντολογικό πλαίσιο συμμόρφωσης με κανονιστικές απαιτήσεις ηλεκτρονικής διακυβέρνησης (EGRRC), το οποίο περιγράφει τις αλληλένδετες έννοιες των κανονιστικών απαιτήσεων στην ανάπτυξη συστημάτων ηλεκτρονικής διακυβέρνησης. Επιπλέον εφαρμόζει την οντολογία

EGRRC στον πρόσφατο Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης (ΕΕ) χρησιμοποιώντας το εργαλείο ανάπτυξης οντολογίας Protégé. Ο ερευνητής και ο επαγγελματίας της ηλεκτρονικής διακυβέρνησης μπορούν να χρησιμοποιήσουν αυτό το πλαίσιο ως αποθετήριο γνώσεων για να διερευνήσουν τις έννοιες της συμμόρφωσης με τις κανονιστικές απαιτήσεις και να κατανοήσουν την επίδρασή τους στην ανάπτυξη του συστήματος ηλεκτρονικής διακυβέρνησης. Οι νομοθεσίες ηλεκτρονικής διακυβέρνησης μπορούν να εφαρμοστούν και να χαρτογραφηθούν στην οντολογία του EGRRC, καθιστώντας την τελευταία μία βάση εξαγωγής γνώσεων σχετικά με την πηγή των κανονιστικών απαιτήσεων, τους στόχους του κανονισμού, τους διάφορους τύπους κανονιστικών απαιτήσεων και τις επιπτώσεις τους στο σύστημα, τις υπηρεσίες που επηρεάζονται από τον κανονισμό, τον προσανατολισμό των κανονιστικών κανόνων στις απαιτήσεις, τις προτεραιότητες των κανονιστικών κανόνων και τις πιθανές τροποποιήσεις των κανονισμών κατά τη διάρκεια ανάπτυξης του συστήματος ηλεκτρονικής διακυβέρνησης.

Επιπλέον, αυτή η μελέτη επιδιώκει την διασύνδεση μεταξύ των εννοιών των κανονιστικών απαιτήσεων ηλεκτρονικής διακυβέρνησης και των εννοιών ανάπτυξης συστημάτων πληροφοριών, γεφυρώνοντας έτσι αυτούς τους δύο τομείς. Σε αυτήν την προσπάθεια, παρουσιάζεται ένα πλαίσιο οντολογίας Ανάπτυξης Πληροφοριακού Συστήματος Συμμόρφωσης (Compliant Information System developMEnT - CISMET) που βασίζεται στην επαναχρησιμοποίηση των εννοιών από την οντολογία EGRRC καθώς και από τις διαθέσιμες οντολογίες στη βιβλιογραφία που περιγράφουν τις βασικές έννοιες της ανάπτυξης συστημάτων πληροφοριών. Χαρακτηριστικές τέτοιες έννοιες είναι οι στόχοι ανάπτυξης του συστήματος, οι υπηρεσίες , οι διαδικασίες, οι δραστηριότητες, τα αντικείμενα και οι πόροι. Έτσι, αυτή η μελέτη βοηθά τον ερευνητή της ηλεκτρονικής διακυβέρνησης και τον προγραμματιστή συστήματος, παρέχοντας μια σαφή κατανόηση των εννοιών της συμμόρφωσης με τις κανονιστικές απαιτήσεις και των συσχετίσεών τους στη διαδικασία ανάπτυξης του συστήματος πληροφοριών. Παρέχει επίσης καθοδήγηση σχετικά με τις τεχνικές τροποποιήσεις που χρειάζονται στην ανάπτυξη του συστήματος ηλεκτρονικής διακυβέρνησης για την προσαρμογή στις νομοθετικές

απαιτήσεις που το επηρεάζουν. Το πλαίσιο παρέχει την ευκαιρία υποβολής ερωτημάτων σχετικά με τις επιπτώσεις της νομοθεσίας στα έργα ανάπτυξης του συστήματος πληροφοριών ηλεκτρονικής διακυβέρνησης, μέσω των υφιστάμενων υφιστάμενων παραδειγμάτων νομοθεσιών (όπως το GDPR, το HIPPA, το σχέδιο δράσης της ΕΕ για την ηλεκτρονική διακυβέρνηση κ.λπ. .) ή μελλοντικές επεκτάσεις στο ολοκληρωμένο οντολογικό πλαίσιο. Για το λόγο αυτό, παρουσιάζεται μια εξειδικευμένη εφαρμογή front-end που μπορεί να βοηθήσει στη διαμόρφωση και την υποβολή αυτών των ερωτημάτων.

Τα στοιχεία οντολογίας εξάγονται εξετάζοντας τις υπάρχουσες οντολογίες, καθώς και τη γενική δημοσιευμένη βιβλιογραφία που παρουσιάζεται στην ηλεκτρονική διακυβέρνηση, τα πληροφοριακά συστήματα και το νομικό πεδίο. Αυτό είναι ιδιαίτερα χρήσιμο για την προσαρμογή στην αρχή των Linked Data, δηλαδή την επαναχρησιμοποίηση, επέκταση και συνδυασμό υπαρχόντων λεξιλογίων από διαθέσιμες οντολογίες, ώστε να αποφεύγεται η επανάληψη υπαρχόντων ορισμών και εννοιών. Η αρχή αυτή εφαρμόστηκε και στις δύο προτεινόμενες οντολογίες (EGRRC και CISMET). Οι τελευταίες ορίζουν νέες κλάσεις υποκειμένων και αντικειμένων όπου χρειάζεται, αλλά κυρίως ασχολούνται με τον καθορισμό νέων σχέσεων (διασυνδέσεων) ανάμεσα στις έννοιες (νέες ή επαναχρησιμοποιούμενες). Στην οντολογία του EGRRC, έχουν εισαχθεί συνολικά 45 νέες ιδιότητες κλάσης μεταξύ των συνολικών 75 σχέσεων που υπάρχουν ανάμεσα σε 42 κλάσεις υποκειμένων και 39 κλάσεις αντικειμένων. Έχουν χρησιμοποιηθεί στοιχεία από 51 οντολογίες της γενικής δημοσιευμένης βιβλιογραφίας στον τομέα της ηλεκτρονικής διακυβέρνησης και των κανονισμών. Στην οντολογία CISMET, έχουν εισαχθεί συνολικά 21 ιδιότητες κλάσης μεταξύ των 44 σχέσεων ανάμεσα σε 24 κλάσεις υποκειμένων και 32 κλάσεις αντικειμένων από 27 υπάρχουσες οντολογίες στον τομέα της βιβλιογραφίας ανάπτυξης συστημάτων πληροφοριών. Επιπλέον, υπάρχουν 82 αρχικοποιήσεις εννοιών (instances) που έχουν εξαχθεί από το κείμενο του ΓΚΠΔ (GDPR) για να χαρτογραφηθούν στις οντολογίες EGRRC και CISMET, στο πλαίσιο επικύρωσης της χρησιμότητας των οντολογιών.

Key Words: Πολιτική και κανονισμός ηλεκτρονικής διακυβέρνησης · Υπηρεσία ηλεκτρονικής διακυβέρνησης; GDPR; Πλαίσιο οντολογίας; Συμμόρφωση με τις κανονιστικές απαιτήσεις. Σύστημα πληροφορίων; Συνδεδεμένα δεδομένα; Ανάπτυξη σχεδίου; Σημασιολογική τεχνολογία.

Abstract in English

E-Government is gaining attention by the researcher and practitioner to digitize the public sector through enacting several policies and regulations. However, the E-Government system development projects often face uncertainties and problems in the grey regulation areas or being constrained by existing regulations in adopting new technologies and solutions for E-Government service development. Moreover, new regulations are also growing in public administration to support the emerging digital government. Hence, the compliance of regulatory requirements from these policies and regulations becomes a liability in E-Government system development. And inadequate understanding of these regulations in E-Government system development often leads to the partial and in some case total project failure. Therefore, the E-Government system development projects have the need for high compliance with existing and/or upcoming regulatory frameworks. However, how a legislation may or may not affect the E-Government information system development projects is often not easily identifiable due to a lack of clear understanding of the regulatory requirements compliance as well as the domain gap between legal sciences, E-Government, and IT. Furthermore, due to the frequent update of legislative content, either in local, regional, or wider levels (e.g., EU level), these aspects need to be identified clearly and their effects be understood in various levels of E-Government information system development.

This study presents an E-Government regulatory requirements compliance ontology framework (EGRRC) that describes the interrelated concepts of regulatory requirements compliance in E-Government system development and discusses the implementation of EGRRC ontology in recently introduced General Data Protection Regulation (GDPR) for personal data processing across countries under the European Union (EU) using the ontology development tool Protégé. The E-Government researcher and practitioner can use this framework as a knowledge repository to explore the concepts of regulatory requirements compliance and understand their interrelationships in the E-Government system development. Furthermore, the E-

Government legislations can be implemented and mapped in the EGRRC ontology that serves as a basis for queries to infer knowledge about the source of regulatory requirements, objectives of the regulation, various types regulatory requirements and their implication in the system, services affected by the regulation, orientation of regulatory rules in the requirements, priorities of the regulatory rules and regulations, and potential amendments of the regulations in the process of the E-Government system development.

Furthermore, this study integrates the concepts of E-Government regulatory requirements compliance to the information system development concepts, thus bridging these two domains. In this effort, this study presents a framework of Compliant Information System developMEnT (CISMET) ontology based on reusing and extracting the definitions from EGRRC ontology and available ontologies in the literature describing the core concepts of information system development such as the system development goals, services, process, activities, artifacts, and resources. Thus, this study aids the E-Government researcher and system developer by providing a clear understanding of the concepts of regulatory requirements compliance and their interrelations in information system development process. It also provides guidance around technical modifications of the E-Government system development to adapt to the legislative actions that affect the IT system development process. Furthermore, it provides an opportunity to allow them to make various queries about the effects of the legislation in the E-Government information system development projects, through the implemented existing example legislations (such as GDPR, HIPPA, EU E-Government Action Plan, etc.) or future extensions into the integrated ontology framework. For this reason, a specialized front-end application is also presented that can aid in formulating and submitting these queries.

The ontology elements are extracted by reviewing the existing ontologies as well as general published literature presented in the E-Government, information system, and legal domain. This is particularly useful in adapting to the concept of Linked Data paradigm in reusing, extending, and combining the existing vocabularies from the available ontologies to enhance their reusability and extension to the EGRRC and

CISMET ontology while avoiding duplication of the existing definitions. The EGRRC and CISMET ontology defines a few subjects and objects class where needed but mainly deals with defining new relationships. In the EGRRC ontology, a total of 45 class properties have been introduced among the 75 relations made between the total of 42 subject classes and 39 object classes from 51 ontologies and general published literature in the E-Government and regulation domain. In the CISMET ontology, a total of 21 class properties have been introduced among the 44 relations made between the total of 24 subject classes and 32 object classes from 27 existing ontologies in the field of information system development literature. Furthermore, there are 82 instances have been extracted from GDPR text to map into the EGRRC and CISMET ontology to demonstrate the usefulness of the ontologies.

Keywords: E-Government Policy and Regulation; E-Government Service; GDPR; Ontology Framework; Regulatory Requirements Compliance; Information System; Linked Data; Project Development; Semantic Technology.

Abbreviations

CISMET	Compliant Information System developMEnT
DSRM	The Design Science Research Methodology
EGDI	The E-Government Development Index
EU	European Union
EGRRC	E-Government Regulatory Requirements Compliance
ICT	Information Communication and Technology
IaaS	Infrastructure as a Service
ISO	International Organization for Standardization
GDPR	General Data Protection Regulation
GLBA	The Gramm-Leach-Bliley Act.
HIPPA	The Health Insurance Portability and Accountability Act.
OECD	Organization for Economic Co-Operation and Development
OWL	Web Ontology Language
SLAs	Service Level Agreements
SLR	The Systematic Literature Review
SOX	The Sarbanes Oxley Act.
XML	Extensible Markup Language

Glossary

Blockchain Technology	Blockchain technology is a system that records information into several distributed blocks which allows the system developer to build an immutable, secure, and publicly accessible data. The blockchain approach can be very useful in creating and maintaining smart contracts or policies with public access in such a way that it will be impossible for the unknown authorities to alter the clause in the contract/policy.
CISMET	Compliant Information System developMEnT (CISMET) is an ontology framework that provide guidance around technical modifications of the E-Government system development to adapt to the legislative actions that affect the IT system development process. It describes the core concepts of information system development from regulatory perspective such as the system development goals, services, process, activities, and resources.
Cloud Computing	Cloud computing is the availability of on-demand computer and information system resources in particular data storage known as cloud storage or data centers available to multiple users over the internet technology. With the use of cloud computing the users can access application and electronic files from anywhere and any devices such as Google's Gmail.
DSRM	The Design Science Research Methodology (DSRM) incorporates necessary procedures, principles, and practices to conduct scientific research through investigating prior literature in order to provide nominal process model of doing research and also provide mental model of evaluation and presenting research outcomes in information system domain.
EGDI	The E-Government Development Index (EGDI) presents the E-Government maturity status of the member countries of United Nations (UN) by assessing their website patterns, infrastructure, and education. This reflects the usage of information technologies among the UN member countries to promote electronic services, communications, and human capacity.
E-Government	Electronic Government in short E-Government is also known as digital government. The primary purpose of E-Government is to deliver public electronic services (e-services) through the use of information and communication technologies such as internet and computers to provide convenient access of public services to the

	citizens, business organizations, and government employees to make the government operations/activities more efficient, reliable, interactive, and transparent.
EGRRC	E-Government Regulatory Requirements Compliance (EGRRC) is an ontology-based framework that describe the interrelated concepts of regulatory requirements compliance in E-Government system development that serves as a basis for queries to infer knowledge about the source of regulatory requirements, objectives of the regulation, various types regulatory requirements and their implication in the system, services affected by the regulation, orientation of regulatory rules in the requirements, priorities, and amendments of the regulations in the E-Government system development.
E-Service	Electronic Service (E-Service) usually refers to the service delivery via any form of ICTs such as the internet, mobile network, television and radio broadcasting to the individual, group or organization at any place (e.g., residence, workplace, public place) in any time (24x7x365) by public or private sectors.
G-Cloud	The Government Cloud (G-Cloud) is a framework where cloud-based solutions provided by suppliers are made available for the government organizations to evaluate and pursue various cloud-based services in place of traditional on-premises based services.
ICT	Information Communication and Technology (ICT) is the extension of Information Technology (IT) usually refers to the internet, mobile network, television and radio broadcasting, as well as enterprise software application, audiovisual systems, and electronic storage that enable its users to store, access, transmit, and modify information.
IaaS	Infrastructure as a Service (IaaS) is one of the specialized form of cloud services implemented with cloud computing in the virtual infrastructure that usually provides the computing resources managed over the internet. The computing resources can be scale up and scale down according to the user's demand and allow them to pay only for what they have actually used.
GDPR	General Data Protection Regulation (GDPR) is the European's digital privacy legislation enacted in 2018 that provides regulatory requirements for personal data processing applies to the organizations across European countries where the data owners have more control over their personal data processing. The European

	Commission has presented the new GDPR regulation which is planned to replace the old Directive 95/46/EC 1995.
GLBA	The Gramm-Leach-Bliley Act (GLBA) of 1999 is a United States federal law to control how the financial institutes should handle the private information of any individuals. The GLBA Act was proposed to update and modernize the existing provisions regarding operations of financial industry operating in the United States.
HIPPA	The Health Insurance Portability and Accountability Act (HIPPA) regulation enacted by the United States government in 1996 which provides privacy requirements for protecting certain health information of the US citizens and security requirements for storing electronic health record and transferring health information through electronic media.
Linked Data	Linked Data plays a fundamental roles in Semantic Web or Web of Data which establish links between various concepts classes and datasets to make it understandable to the humans and machines. And the Linked Data provides a set of design principles that encode statements into triples to share the interlinked machine-readable data on the web.
Ontology	In the domain of information and computer science, an ontology represents and defines various concepts and properties to define relationships between various concepts. Ontologies are frameworks that represents reusable and sharable knowledge to describe their classification and taxonomies in defining knowledge structure in the information domain.
OWL	Web Ontology Language (OWL) is semantic web knowledge representation language for defining ontologies in the web. In semantic web , OWL has been designed to describe and represent a knowledge domain in terms of classes, properties, and individuals of the web resources.
Semantic Web	Semantic Web is an extension of current world wide web where the information is represented with well-defined structure and their meaning in the web pages so that it can be readable by the machine. It enables the humans and computers to work in co-operation.
SLA	Service Level Agreements (SLAs) defines a contract that establishes the customer expectations of service level from the supplier where a set of service deliverables has been agreed upon the supplier and customer. The SLAs are usually signed off between an organization

	and its external supplier or customers, but two departments in an organization may have service level agreement between them.
SLR	The Systematic Literature Review (SLR) uses systematic methods and techniques to identify, select, and critically evaluate secondary data from published literature in order to answer the defined research questions. It provides a comprehensive and exhaustive qualitatively and quantitative findings regarding broad or narrow research scope with their evidence.
SOX	The Sarbanes Oxley Act (SOX) is a federal regulation enacted in the United States in 2002 that sets standards for audit reporting in the public and private organizations to ensure data accuracy.
Regulatory Requirements	The regulatory requirements are any applicable laws, rules and regulations, guidelines, contracts, and standards from any regional, state, national, or international authorities that apply directly or indirectly to govern the organizations, business, products, services, operations, etc.
Requirements Compliance	The compliance is related to the actions regarding compliance with the requirement. In information system, the Requirements compliance process ensures that the information system project development and its operations are in accordance with prescribed guidelines and/or agreed set of rules defined in related regulations, laws, policies, standards, and any ethical practices followed by the organizations.
XML Schema	XML Schema specifies the elements, attributes, and data types presented in the Extensible Markup Language (XML) document. It is commonly used to describe the structure of an XML document. In particular, XML Schema is used to express the constraints as well as describe and validate the structure and content of the XML data.

Chapter 1: Introduction

"Research is formalized curiosity. It is poking and prying with a purpose."

- Zora Neale Hurston

1.1 E-Government Service Development

With the unprecedented opportunities of information technology, the revolution of the modern world is now focusing on the information age from industrial age. And the manifestation of this transformation is emerging in the field of electronic services (E-Service) such as e-Government, e-Commerce, e-Business, e-Mail, e-Learning, etc. which have become a part of our daily lives (Almarabeh & AbuAli, 2010). The electronic service often called e-service is the benefit available via Information and Communication Technologies (ICTs) to create new efficiencies in the daily life and drive new revenue streams to the public and private organizations (Piccinelli & Stammers, 2002).

Although, some definitions of electronic service tend to restrict e-service to only the internet-enabled applications, however, electronic service usually refers to the service delivery via any form of ICTs such as the internet, mobile network, television, and radio broadcasting to the individual, group or organization at any place (e.g., residence, workplace, public place) in any time (24x7x365) by public or private sectors (Gouscos et al., 2001; Scupola et al. 2009). For example, buying and selling over the internet, online information sharing and collaboration, electronic health application, electronic money transaction, and many more.

The electronic services provided by the government agencies to its employees, citizens, business organizations are known as E-Government services often called public e-service. E-Government service first came to Europe during the late 1980s. In order to link remote villages with the central government, a few European countries introduced "Electronic Village" known as Electronic Government. However, United States (US) government formally introduced public e-Service to the citizens in 1993 (Alasem, 2009). E-Government is an idea raised by the government of the United States within the vision of linking the citizens to the various government agencies for getting all the services provided by the government in an automated and automatic way (Almarabeh & AbuAli, 2010). The E-Government is defined as an electronic form of government that comprises alignment of IT infrastructure, business process and service content in order to provide high-quality and value-added electronic services to the employees of the government agencies, citizens, and business organizations (Gouscos et al., 2001).

Within three decades, E-Government is now recognized as one of the most vibrant fields of research and practice in the context of public sector modernization where e-service is considering as the key branch of E-Government in research and practice (Wimmer et al., 2008; Lofstedt, 2012). Many governments of the developed countries have already taken progressive steps toward the use of ICT in various government agencies at the central and local regions. This will widen the local access and skills of information usage, add coherences to all the government activities and open interactive services which increase the participation of the citizens and business organizations with the government agencies (Graham & Aurigi, 1997).

The implementation of the E-Government system in public organizations is an evolutionary phenomenon. The continuous process of E-Government development is often conceptualized in several phases. The wildly known E-Government maturity model proposed by Layne & Lee (2001) explains the E-Government initiatives into four stages in terms of complexity involved in different levels of service integration starting from simple and sparse to the complete and complex E-Government system. The initial initiative of E-Government system development is only limited to the one-way communication for the online presence of government information in electronic documents on their designated websites. The initial phase of E-Government is also known as the cataloguing stage because the primary effort of E-Government development is to organize and make accessible the scattered electronic documents and forms to the citizens and business organizations through government official websites. The second initiative of E-Government development is focused on providing the citizens and business organization an online interface to interact with the government electronically. This phase is also known as the transaction stage of E-Government development because the E-Government effort is to provide an online interface of the database, so that, the citizens can make the online transactions, for example, pay utility bills and tax through online, make payment for passport issuing, renewing the driving license, etc.

With the improvement of e-transaction qualities, the E-Government systems are forced to integrate the internally functional intranet among various government agencies into the central state level E-Government system in order to provide one-stop E-Government services to the citizens and business organizations. The actual benefit of implementing a one-stop E-Government system is to derive e-services not only from different levels of government agencies but also from different job functions across government agencies. By having this one-stop E-Government service, a citizen may contact one point of the government agencies and shall be able to complete his/her tasks and get desire services without roaming around different levels of government offices and their varieties of job functions. Furthermore, the ubiquitous government services and integrated information base is a way to eliminate the redundancies of information across various government agencies and also maintain consistency of the information.

The service integration for one-stop E-Government service delivery may happen in two different ways. The vertical integration assimilates the E-Government service derived across local, state, and federal levels of government. For example, when a citizen files an application for a business trade license at the municipality office, the information recorded in the file would be propagated to the business trade licensing system at the state government and federal government in case of obtaining the employer identification number for any use. Another example of vertical integration in E-Government service is the user of the national crime databases. Any crime information from the local crime database is forwarded to the state government for analyzing the compliance of rules and order enacted by the government and forward the statistics of criminal activities to the federal government for necessary policymaking. In contrast to vertical integration, the horizontal integration assimilates the E-Government services across different functions of the government operations. For example, the unemployment insurance of a citizen is paid in one state agency and the citizen pays taxes to another agency and these two agencies are working together in a single database to process the citizen information.

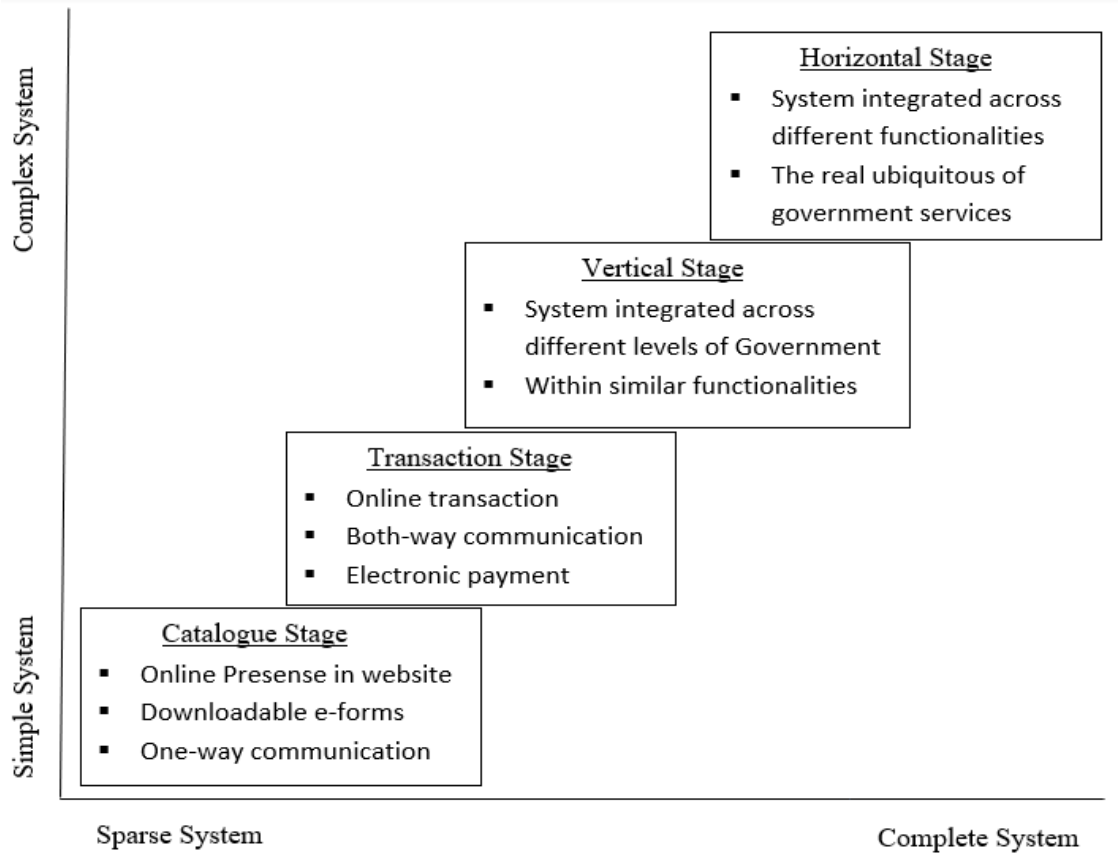


Figure 1: The Maturity of E-Government Systems

Moreover, among the multiple solutions varying in the efficiency and the degree of reliability in information transactions in E-Government systems, the blockchain technology shows promising potential in recent E-Government system development,

mainly for validating and displaying document history. It provides a data exchange platform that facilitates interlinked data generation by various government authorities without making any replica and ensure reliable information exchange among different authorities connected to one another. For example, the police agencies constantly require data from the population register while the unemployment insurance fund depends on the information from the health information system (Markusheuski et al., 2017; Rahmadika & Rhee 2018).

Furthermore, in Greece and other European countries, the cloud computing concepts become an integral part of the national digital strategy and E-Government action plan regarding public sector modernization to enhance the E-Government initiatives. For example, in recent times the Government Cloud (G-Cloud) initiatives taken by Greek public administration reflects the strategic reforms of public sector modernization in Greek E-Government service delivery to the citizens and business organizations. In the E-Government operation, G-Cloud technology offers high-quality services in line with the Service Level Agreements (SLAs) based on the state-of-the-art cloud computing virtual technologies such as Infrastructure as a Service - IaaS (European Commission, 2019). The objective is to provide various government agencies with the ability to use virtual servers or machines to fulfil their needs of operating in a managed and secured centralized environment. The joint use of IT infrastructure by various government agencies provides them the opportunities to reduce the cost of acquiring and maintaining the system operations. Also, improve the service quality and provide greater flexibility in a manageable and stable computing environment and security in E-Government service delivery to the citizens and business organizations (G-Cloud, 2020). For example, the Greek public administration has already implemented the G-Cloud based integrated healthcare information system to provide allowance (in total 680M€ annually) to the healthcare subsidies over 200,000 beneficiaries through 1400 active users of the government employees across the municipal and regional authorities (Nanos et al., 2017).

The objective of E-Government system development is to achieve greater efficiency in public service operations by improving the performance of government services delivered to all segments of service recipients (Middleton, 2007). Furthermore, E-Government makes the government more efficient in administrative work and transparent towards developing trust in government in their functions. It delivers government services to the citizens in much easier and faster media where the service recipient does not need to visit different offices of the government agencies and waiting in the queue for their desire services. Through the E-Government, the one-stop e-services are brought to the citizen’s convenient place such as the home, office, or any other location where a mouse click will do the same work of queuing at the different government offices for all day long (Anna Xiong, 2006). Moreover, one of the main reasons for implementing E-Government systems in developed countries is to reduce the cost of information processing and service delivery through online transactions (Dada, 2006).

1.2 Regulatory Requirements in E-Government Service

Now-a-days, the E-Government system is developed within the scope of growingly regulated environments and every system development, therefore, must ensure the obligations described in laws and regulations enacted by multiple authorities (Massey et al., 2014). The regulatory requirements are any applicable laws, rules and regulations, guidelines, contracts, and standards from any regional, state, national, or international authorities that apply directly or indirectly to govern the organizations, business process, products, services, operations, etc. (Law Insider, 2020). In the E-Government service development, regulatory requirement means the guidelines agreed by the respective authorities to develop the E-Government system, operate the E-Government system to deliver service, and provide access of E-Government services to citizens and business organizations. For example, the stakeholder rights and obligations are prescribed by the federal and state regulations that must be satisfied by the system requirements (Breaux et al., 2006). Following table discusses some of the regulations and their applicability in identifying regulatory requirements in E-Government service development.

Table 1: Regulations and Regulatory Requirements Objectives

Regulation Name	**Regulatory Requirements Objectives**
GDPR - General Data Protection Regulation (EUROPA, 2018)	The GDPR is the European's digital privacy legislation enacted in 2018 that provides regulatory requirements for personal data processing applies to the organizations across EU countries where the data owners have more control over their personal data processing. The objective of GDPR is to protect the rights of using individual's personal data and facilitate the exchanging of personal data within EU member states through a uniform legislation towards advancing the digital agenda and economic growth across EU countries.
European E-Government Action Plan (EUROPA, 2019)	The European E-Government Action Plan 2016-2020 is setting the policy for digital single market strategy for Europe. The objective of the action plan is to make the public administration of European countries more open, efficient, and borderless in providing digital public services to all the citizens and business organizations.
HIPPA – Health Insurance Portability and Accountability Act. (HHS.Gov, 1996)	The HIPPA regulation enacted by the United States government in 1996 which provides privacy requirements for protecting certain health information of the US citizens and security requirements for storing electronic health record and transferring health information through electronic media.
ISO/IEC 27001 – International Security Standard (IT	The ISO/IEC 27001 established in 2013, is the international security standard that sets the requirements for Information Security Management System (ISMS). The ISO27001

Governance, 2013)	regulation helps the organizations in managing their information security issues while protecting confidential and sensitive personal data from being destroyed or exposed to unauthorized access.
SOX - The Sarbanes-Oxley Act (SOX Law, 2002)	The SOX is a federal regulation enacted in the United States in 2002 that sets standards for audit reporting in the public and private organizations to ensure data accuracy. The SOX regulation ensures the adequate controls of storing and safeguarding the electronic data in an organization and make transactions over secured electronic media.
GLBA – The Gramm-Leach-Bliley Act (FTC.Gov, 1999)	The Gramm-Leach-Bliley Act (GLBA) of 1999 is a United States federal law to control how the financial institutes should handle the private information of any individuals. The requirement from the act says that the financial institutes must provide the security of confidential customer records and protect their confidential information from any unauthorized access.
FCT – Fair Credit Reporting Act (FTC.Gov, 1970)	The Fair Credit Act (FTCA) enacted by the United States Federal Government regulations enacted in 1970 to protect the privacy of consumer information and promote fairness and accuracy of information collection, dissemination, and usage by consumer reporting organizations such as medical center, credit bureaus, tenant screening services, etc.

Furthermore, almost all of the nationals across the continents also come forth with several policies and guidelines of E-Government action plan to modernize the operations of their public administration to provide effective and efficient electronic services to the citizens and business organizations. For example, The United Republic of Tanzania published an E-Government guideline in 2013 on how to leverage ICTs in improving the service delivery process and provide quality, effective, and efficient e-services to the Tanzanian citizens and business organizations operating in Tanzania (Public Service Management, 2017). The Socialist Republic of Vietnam has devised the E-Government policies that provide guidelines in the modernizing process of public administration offices using ICT infrastructure such as tax administration, customs management, population management services (DO LAP HIEN, 2017). The Republic of Singapore provides the policy of eGov2015 Masterplan to establish an interactive infrastructure environment of a collaborative government where the government, private sectors, and the people can work together seamlessly to produce new value-added one-stop public electronic services (Ministry of Finance – Singapore, 2015). We can go on and on discussing the countless number of E-Government system development policies and guidelines set out for each and every nation across the continents and various administrative departments of a country.

The growing number of policies and regulations have been affected the countries all over the world to embrace and enhance E-Government solutions in providing public services to the citizens and business organizations. In the year 2019, total 44% of the EU citizens reported that they have received information and services from public organizations during the last 12 months which as just 33% in 2008. Among the European countries, particularly the Nordic countries are fast forward in using E-Government services, for example, 89% of citizens from Denmark, 84% of citizens from Finland, and 79% of citizens from Sweden have received E-Government services during this period (EUROSTAT, 2020). The United Nation's survey in 2020 reflects the global E-Government development trends and improvement of public e-service delivery through quality of e-services, ICT infrastructure, and human capacity. The UN survey of E-Government Development Index (EGDI) rank reveals that many countries are transitioning from lower to higher level of EGDI in the year 2020. In this survey edition, total of 57 countries among the UN Member states have achieved very high EGDI index value between 0.75 to 1.00 in terms of digital government let by Denmark, Korea, Estonia, Finland, Australia, Sweden, UK, New Zealand, USA, Netherlands, Singapore, Iceland, Norway, and Japan. Among the least developing countries like Bhutan, Bangladesh, Cambodia become the leaders in E-Government development in 2020's UN survey and advancing from middle to high EGDI index level. And South Africa is the leading country of E-Government development in Africa. It is apparent from the survey that all regions are making progress in E-Government development where Europe remains the leader with 58% of the high EGDI indexed countries, followed by Asia 26%, Americans 12%, and Oceania 4% of high EGDI index level (UN Report, 2020).

Along with the advancement of E-Government development across the continents, there are some significant challenges and loopholes become obvious to be considered in research and practice. The primary challenges are the privacy and security concerns as many regulations and standards have been enacted discussed in Table1 to protect individual's confidential information in E-Government service development. Furthermore, the Organization for Economic Co-Operation and Development (OECD) reported that the contemporary E-Government is facing challenges of incompatible, confusion, and overlapping proliferation of websites among the government agencies where the Government cloud (G-Cloud) solutions also become hinder because of the constantly growing and changing regulatory landscape environment from multiple authorities (OECD, 2020). Some other challenges of E-Government service development, in general, are the difficulties in implementing E-Government guidelines, lack of compatibility in integrating E-Government systems, lack of understanding of system development regulations and policies, obscure privacy and security issues in recording and transacting digital data, conflicts of data ownership and data control etc. (Al-rawahna et al., 2019). In today's digital information age, these challenges regarding electronic service development make the E-Government regulatory requirements a pivotal point of research contribution.

1.3 Research Background and Motivation

Although in this globalization era the electronic operations of government and business organizations are expanding rapidly to cope with the technological advancement, however, the recent corporate history provides the evidence of some largest disasters and scandals in business organizations because of the lack of control over the electronic operations. Insecure financial transactions, unauthorized information access, fraud identity, etc. are the few examples behind this crisis (Chun, 2019; Syed, 2019; Sadiq et al., 2007).

To protect the vulnerability of electronic transaction and ascertain the control over the electronic operations, several national and international regulations have been enacted and obliged in the organizations some of them are discussed in Table 1 (Maxwell et al., 2012; Maxwell & Anton, 2010). Regulatory requirements compliance essentially means ensuring that the system development and its operations are in accordance with prescribed guidelines and/or agreed set of rules. The introduction of regulations such as General Data Protection Regulation (GDPR), Sarbanes Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLB) have made the regulatory requirement compliance a pivotal point of information system research and development activities since non-compliance to the regulatory requirements of these regulations can have dire consequences (Abdullah et al., 2009). Regulatory requirement compliance has become a critical concern nowadays for public and private organizations since failing to comply with the regulations is no longer an option (OECD, 2020; Al-rawahna et al., 2019; Anon et al., 2007). The organizations are increasingly concerned with high investment for compliance management emerged as a result of events that led to some of the largest disasters in the corporate usage of information technology, such as the Cambridge Analytica case of 2018 (UK) , WorldCom, Tricare, Choice Point (USA), HIH (Australia), Société General (France) (The Guardian, 2018; Braganza & Franken, 2007; Bace et al., 2006). Furthermore, in the current globalized ecosystem via the use of distributed computing resources such as cloud solutions provides cross-border e-services offer by various information systems often amplifies and complicates the regulatory environments of what rules to apply, in which cases, for which roles and subjects (Khan et al., 2019; Nanos et al., 2017).

Information system development projects often face uncertainties and problems in the grey regulation areas or are being constrained by existing regulations in adopting new technologies and solutions for new service development. Moreover, organizations are now facing difficulties to comply with a rapidly growing number and increasing complexities of new regulations, and standards. This has a significant impact on how the organizations develop an information system and adapt changes to its operations with the compliance of regulatory requirements (Yoon, 2018; Cleven & Winter, 2009; Alpar & Olbrich, 2005). Therefore, the IT professionals are facing problems more than ever to ensure that the system development complies with relevant regulations

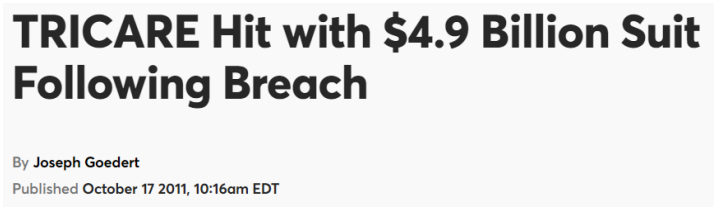
enacted by local, state, region, and even international policies and regulations. The costs of non-compliant system development may cause loss of trust, reputation, and enormous amount of financial burden (Maxwell et al., 2012; Breaux & Anton, 2008).

For example, ChoicePoint Inc. founded in 1997 is one of the largest data broker organizations operating across the states in the United States. It acted as a private intelligence service provider to the government agencies, business, and non-profit organizations in providing a wide range of e-services based on personal information such as background screening, authentication of public records, marketing services, etc. The main business of ChoicePoint is driven by information transactions such as information screening for pre-employment of applicants in an organization or the processing insurance files. The majority of these information transactions are regulated by the Fair Credit Reporting Act (FCRA) enacted by Federal Government legislation to promote fairness, accuracy, and privacy of personal information contained in consumer reporting agencies (Culnan & Williams, 2009). In Figure 2, on October 20, 2009, Mills (2009) reported that the company failed to implement a secured information system in protecting the sensitive information of the citizens and left the door open to a data breach of personal information of 13,750 people which put them at risk of their identity theft by the unauthorized entity. The Federal Trade Commission (FTC, 2009) charges ChoicePoint data breach which costs the company over 27 million dollars and in addition causes loss of reputation, brand damage, employee retraining and having government audits for 20 years for allowing unauthorized access and exposing confidential information (Maxwell et al., 2012; Maxwell & Anton, 2010).

Figure 2: ChoicePoint Data Breach (Mills, 2009)

Another example of the regulatory requirement non-compliance is the TRICARE data breach. The TRICARE is a health care program of the Department of Defense Military Health System operating in the United States. It provides health benefits for active military personal, retirees and their dependents. In Figure 3, on October 14, 2011, Vijayan (2011) reported that a $ 4.9 billion lawsuit was filed against TRICARE for the theft of unencrypted backup tapes used to store personal confidential information of millions of individuals. The lawsuit was filed in the federal court of Washington D.C. by four victims whose data was compromised violating the privacy rights of information including names, addresses, social security numbers, phone numbers, personal health information. The lawsuit charges the Tricare organization

with $1000 for each of the 4.9 million individuals may have affected by the data breach (Maxwell et al., 2012).



TRICARE Hit with $4.9 Billion Suit Following Breach

By **Joseph Goedert**
Published **October 17 2011, 10:16am EDT**

Figure 3: TRICARE Data Breach (Goedert, 2011)

Another example of the costly penalties of regulatory requirements non-compliance is the Stanford Hospital data privacy case. Stanford Hospital is the most prestigious medical center in California. According to the world report it has been consistently ranked as one of the best hospitals in the United States. It also serves as one of the primary teaching institutes for the School of Medicine at Stanford University. In Figure 4, on October 5, Sack (2011) reported that the confidential information of about 20,000 patients has been posted on their public website and remains there for nearly a year. As a consequence, the Stanford Hospital was given a penalty of $20 million lawsuit because of the unauthorized disclosure of protected health information of a number of patients in their public training website (Maxwell et al., 2012).

The New York Times

Patient Data Landed Online After a Series of Missteps

By **KEVIN SACK** OCT. 5, 2011

Private medical data for nearly 20,000 emergency room patients at California's prestigious Stanford Hospital were exposed to public view for nearly a year because a billing contractor's marketing agent sent the electronic spreadsheet to a job prospect as part of a skills test, the hospital and contractors confirmed this week. The applicant then sought help by unwittingly posting the confidential data on a tutoring Web site.

Figure 4: Stanford Hospital Data Breach (Sack, 2011)

It is obvious from the example cases discussed above that the organizations of the above examples have given such expensive consequences for not being compliant with the enacted regulations and policies. More precisely, the regulatory requirements that existed in the regulation and policy documents were not fully taken into consideration in the system development. The organizations had ambiguous understanding of regulations and difficulties in inferring the regulatory requirements from various regulations in managing compliance in their information system development (OECD, 2020; Al-rawahna et al., 2019).

1.4 Research Objective

Simple, convenient, and effective interaction between the citizens and government agencies in public service has become a common expectation in the modern information society. Hence, the E-Government solution brings fundamental changes in the traditional government operation that affects the infrastructure of public service delivery. However, the E-Government projects often face uncertainties and problems in the grey regulation areas or are being constrained by existing regulations in adopting new technologies and solutions for E-Government service development. Moreover, new regulations are also growing in public administration to support the emerging digital government. Inadequate understanding of these regulations in E-Government service development often led to the partial and in some case total project failure (Alpar & Olbrich, 2005; Yoon, 2018; Al-rawahna et al., 2019).

The E-Government service development projects have the need for high compliance with existing and/or upcoming regulatory frameworks. However, how a legislation may or may not affect the E-Government system development projects is often not easily identifiable due to lack of clear understanding of the regulatory requirements compliance as well as the domain gap between legal sciences, E-Government, and IT (Soliman et al., 2020; Hale & Gamble, 2019). Furthermore, due to the frequent update of legislative content, either in local, regional, or wider level (e.g., EU level), these aspects need to be identified clearly and their effects be understood in the various levels of E-Government system development. Literature suggests that organizations struggle with finding the proper guidelines, tools, and methods/frameworks for understanding compliance management in E-Government system development for assistance in their compliance management activities (Mustapha et al., 2020; Zarrabi & Tawil, 2019; Anadiotis, 2018). There is a vacuum of research for helping the system developer to clearly understand the regulatory requirements and their effects in the E-Government system development process. The absence of a regulatory requirements framework forces the system developer into the high risk of uncertainties in complying regulatory requirements in E-Government system development process. In the project management tasks, working without a proper framework is like going inside a dark cave without taking a light, where you are bound to get lost. Hence, there is a significant need of a framework that organizes, structures, and describes the interlinked concepts of regulatory requirements to understand their effects and ensure their compliance in the E-Government system development process (OECD, 2020; Al-rawahna et al., 2019).

Moreover, the literature discussed in section 1.5 suggest that compliance management does not seem to be one of the main focus of contemporary E-Government and information system research and practice in providing guidelines towards the E-Government information system development process. It is also reported in some recent literature that there is a need for a comprehensive framework that discusses the compliance of the regulatory requirements in providing necessary technical guidelines

to the IT professionals thought the process of E-Government and IT system development projects (Saidane & Al-Sharieh, 2019; Zarrabi & Tawil, 2019; Anadiotis, 2018). Hence, the apparent lack of guidance for the IT professionals in system development process motivates us to develop a comprehensive framework that describes the regulatory requirements compliance in the E-Government system development projects. The research questions of this study are:

RQ1: How the regulatory requirements compliance is linked with E-Government domain?

RQ2: And how it describes the regulatory compliant tasks and properties of E-Government Information System development project?

In order to operationalize the first research question, the objective of this study is to introduce an E-Government regulatory requirement compliance (EGRRC) ontology framework that describes the interrelated concepts of regulatory requirements compliance in E-Government system development based on the review and reuse of existing works in the E-Government domain in the form of a suitable description schema in knowledge representation. In particular, the EGRRC ontology framework will describe the sources of E-Government regulatory requirements among various types of regulations scattered in local, regional, or wider level. The defined objectives and goals of the regulations onto the regulatory requirements and its various types of categorizations to properly identify the regulatory requirements in the E-Government system development. Also, the framework will describe the types of E-Government services affected by the regulations and formulation of regulatory rules in the requirements to clearly understand their components and associations in the E-Government system development. Furthermore, to describe the prioritization of the E-Government regulatory requirements as every requirement does not have same level of priority to be compliant in the E-Government system development, as well as the maturity of the regulatory requirements as some regulations may change over time, place, and context. Therefore, the E-Government system development needs to understand and prepare for potential amendments of regulatory requirements that eventually lead to the modification in the E-Government systems.

There are several methods that can be used for knowledge representation in various application domains. An XML schema can be used to describe the structure of a legal document that can be machine-understandable and automatically processed for meeting legal requirements in the manipulation of data, for example, in cloud federation scenarios (Kousiouris et al., 2013; Corrales et al., 2017). However, both XML schemas as well as blockchain approaches, while feasible to be used during runtime of the system, they cannot efficiently capture dependencies between concepts during the design time in order to guide developers, nor leverage inference capabilities based on the concept structure. Hence, for the purpose of this study, the OWL ontology is suitable to describe existing concepts from the systematic literature review of related works on existing E-Government and Information System

ontologies in order to enhance the reusability and extension of descriptions for regulatory requirements compliance in E-Government system development (Alexopoulos et al., 2007). Ontologies are a widely accepted knowledge representation paradigm in several application domains and becoming popular in the E-Government system development domain in knowledge management and representation. Ontology is an essential tool for knowledge representation in various domain in establishing domain concepts with well-defined terminologies, definitions, and their interrelationships (Yang et al., 2019; Kendall & McGuinness, 2019).

Furthermore, in order to operationalize the second research question, the objective of this study is to integrate the concepts of E-Government regulatory requirements compliance (EGRRC ontology) to the information system development project, thus bridging these two domains. The study proceeds with the use of the entities defined in the EGRRC ontology and combined them with the core concepts of information system development project and links them in order to assist in the detection of compliance related actions needed in parts of the E-Government information system development project. Although, there are several ontologies and taxonomies that exist in the information system domain, there is lack of a comprehensive framework that describes the technical guidelines of system development projects explained in Section 1.5 of existing ontologies and frameworks. Therefore, the study firstly presents a Compliant Information System developMEnT (CISMET) ontology based on reusing and extracting the definitions from available ontologies in the literature adapting the concepts of Linked Data paradigm (Polleres et al., 2020; Kalampokis et al., 2019, Färbe et al., 2018; Bizer, 2009). The CISMET ontology describes the core concepts of information system development from existing ontologies (Table 1) also suggested in the IT project management practices (Olson, 2020; Hartley, 2018; Pressman, 2014) such as:

- The goal of information systems development that describes the specific objectives
- The process that describes the systematic phases of system development
- The service concepts, describing the e-services provided by the system
- The activity that describes the set of tasks or permissible actions required to be performed in the system development
- The artifact that describes the work products delivered by the activities in the process
- The resource concept that describes the required resources to carry out the system operation and system development activities

Finally, the CISMET ontology is integrated with the EGRRC ontology and define the system development goals, services, process, activities, and resources by using class entities of the EGRRC ontology in order to describe the information system development projects in a combinational manner with the regulatory compliance

concepts. Thus, this study aids the E-Government researcher and system developers by providing:

- A clear understanding of the concepts of regulatory requirements compliance and their interrelations in E-Government information system development
- A guidance around technical modifications of IT system development to adapt to the legislative actions that affect the E-Government system development
- An opportunity to allow the system developers to make various queries about the effects of the legislation in the information system development projects, through the implemented existing example legislations (such as GDPR, HIPPA) or future extensions into the integrated ontology framework. For this reason a specialized front-end application is also presented that can aid in asbtractively formulating and submitting these queries.

1.5 Related Works

There are several research works have been presented in the E-Government and regulatory domain. The E-Government project monitoring ontology is presented by Dombeu (2010) in support of E-Government initiatives for monitoring the project activities performed by various stakeholders involved in the project and facilitating communication among all the stakeholders in the project development. The web content (WC) ontology presented by Thomas & Elnagar (2018) discuss the formal process of concepts and functions representation regarding web content evaluation of the government websites in order to improve the quality of the web content and enhance the evaluation efficiencies. The E-Government Project Management (eGPM) Ontology presented by Sarantis & Askounis (2009) describe the concepts of E-Government project management in support of the stakeholder in keeping contact, sharing resources, approaches, solutions, and problems encountered in implementing the E-Government projects. The Core E-Government ontology presented by Amalanathan (2015) describes an evolutionary method to extend the interoperability of the core E-Government services. The Public E-Government Service (OntoAL) ontology presented by Shehu & Xhina (2019) describe the e-service structure in Albanian E-Government system development. It provides meaningful E-Government services to its citizens based on the enacted regulations towards introducing the digital e-Albania. The E-Government Quality of Service (e-GovQoS) ontology presented by Corradini et al. (2006) discuss the E-Government services and their related quality in promoting the interoperability among the E-Government services provided by multiple public administrations satisfying the quality goals. The E-Government System Quality (QeGS) ontology presented by Magoutas et al. (2007) describe the evaluation of E-Government service quality that enables the E-Government user to assess service quality with a comprehensive and holistic view. The E-Government Goal (e-GovGoal) ontology presented by Salhofer et al. (2009) describe the goal-oriented discovery of e-services provided by the public administration. The SQS

ontology presented by Okike (2017) discusses a three-stage model for the evaluation of software applications in terms of standardization, quality, and services developed by the E-Government project from the E-Government user's perspective.

The process and compliance ontology presented by Schmidt et al. (2007) describe the interactions between the E-Government service providers, customers, and third-party contractors by event-condition-action rules. It also defines various kinds of rules in the E-Government service process. The EGO and EgoIR ontology presented by Ortiz-Rodríguez & Villazón-Terrazas (2006) describe the real-estate transactions within the Spanish Government domain. The main goal of this ontology is to represent a part of the legal processes carried out within the government for integrating and recovering legal documents. The Security ontology presented by Karyda et al. (2006) address the issues related to accommodating security requirements in E-Government applications which can help the developers in making design decisions for fulfilling security requirements more effectively in E-Government system development. The Service evolution ontology presented by Apostou et al. (2005) address the modeling of E-Government services that will facilitate the consistent configuration and re-configuration of E-Government services due to the change in the regulations. The E-Government service ontology presented by Stojanovic et al. (2004) describe the e-services offered by the E-Government system in maintaining the consistency of service description for change management in E-Government. The e-Service ontology presented by Vassilakis & Lepouras (2006) discuss the concepts of administrative responsibilities and legislation in E-Government service. The E-Government Business Knowledge Modelling (EGBOnt) ontology presented by Xiao et al. (2007) describe the business process in government services based on the logic presented in business and civil servant policy. The compliance management ontology presented by Stratigaki et al. (2016) describe the elicitation of various business processes from the regulatory documents in the case of E-Government system development. The E-GIF ontology presented by Fragkou et al. (2014) describe the interconnected concepts available in the license provisions of Greek administration.

The public administration is highly governed by policy and regulation. Hence, the ontologies presented in the regulation domain also considered in the E-Government system development. Cherouana et al. (2019) discuss an ontology approach regarding semantic government process management (SGPM) that can be useful in designing and deploying the government process with legal compliance. The legislative ontology presented by Costilla et al. (2005) discuss the taxonomy among legislative concepts. The policy domain language ontology presented by Barrett et al. (2007) describe a domain ontology for policy representation in order to represent all the policy rules in a common structure. The Genpol policy wizard ontology presented by Campbell (2006) discusses the core structure to describe constraints which are useful when interpreting the policy language. The generic regulation ontology presented by El-Kharbili & Stolarski (2009) discuss the norms and rules in a policy document in order to model policy-based regulations for compliance checking. The OGDL4M

ontology presented by Mockus & Palmiran (2017) discuss the common or open government data licenses framework for a Mash-up Model in order to improve the accuracy level of legal annotations regarding Linked government datasets while connecting the legal rules with the official legal texts for legal expert's use.

Furthermore, there are several studies discuss policy and regulation in the information system development domain. Abdullah et al. (2010) discuss the primary challenges in managing regulatory compliance in information systems development industry, derived from expert interviews, such as lack of compliance knowledge base, frequent changes in regulation, lack of efficient compliance management and understanding of its relevance to the organizations. Mutimukwe et al. (2019) discuss the international privacy standard and practice for the E-Government system development in African countries, Ruhode (2016) discuss ICTs policies of Zimbabwa's government towards developing E-Government System. Rehman et al. (2018) discuss the United Nation's sustainable development goals in E-Government system development. Boella et al. (2013) discuss the legal knowledge management system workflows with the involvement of different roles in the organization to interpret various rules in business process management systems. Muthuri et al. (2017) presents a legal interpretation model to interpret legal provisions in determining business process compliance. Cleven & Winter (2009) provide an overview on the legal and regulatory compliance of information systems from a literature analysis. Wang et al. (2020) discuss the Even-Condition-Action (ECA) rule in E-Government system development. Ingolfo et al. (2011) discuss an argumentation framework that systematically captures the compliance arguments and arguing through a discussion among the involved stakeholders in revising software requirements in order to establish their acceptability for regulatory compliance. DeVos et al. (2019) presents ODRL, an Open Digital Rights Language profile to capture semantics of the policies for business process compliance checking. Siena et al. (2010) discuss a goal-oriented framework to model the healthcare information system domain based on stakeholder actors in the domain in terms of their goal, tasks, quality aspects, and strategic dependencies among the actors in the system to be compliant with a specific law.

Furthermore, Hale & Gamble (2019) presents a semantic hierarchy based stepwise process to extract security provisions from security control standards in preparing service agreements for organizations. Sulistiyani & Susanto (2018) discuss the efficient change management process of E-Government system development due to policy and regulation amendments during and after the E-Government system development. Soliman et al. (2020) discuss semantic based framework to systematically classifying regulatory information for automated rule checking purpose. Xu & Cai (2019) presents a semantic frame-based method for extracting information based on lexical semantics and domain semantics using natural language processing and machine learning techniques. Giblin et al. (2006) describe the rule patterns that occur in high-level regulations to automatically identify and capture the low-level event correlation rules with the help of temporal rule patterns to sensibly

monitor the event correlations as a process of generating runtime artifacts from the high-level policies and regulations. Zhang & El-Gohary (2016) presents a rule based natural language processing approach to automatically process the regulation documents for pattern matching in information extraction. However, it is reported in the literature that the instead of a fully automated process, the semi-automated process of regulatory information extraction from the regulatory documents often may provide greater performance as most of the regulations rely on the subjective nature of the regulation context (Soliman et al., 2020).

Furthermore, in the information system development domain Leppanen (2006) presents ISD ontology that discusses the concepts, relationships, and constraints referring to the purposes, actors, actions, and objects in information system development. Tebes et al. (2020) present TestTDO ontology defines various terms, and their properties and relationships in support of achieving the software development goals through testing activities and quality assurance of software engineering process. Stumpe (2018) presents project system ontology that discusses the influences of project objectives and goals in the project development environment for their application in complex situations. The Strategic Rational i* ontology presented by Beydoun, et al. (2014) also describe the relationships between various goals, tasks, and actors in the system development. Oveh & Egbokhare (2020) discuss software process ontology that presents various process and sub-process in software development activities. ODYSSEY ontology presented by Olszewska & Allison (2018) discuss the Software Development Lifecycle (SDLC) phases which allow the software developer to select and use software development activities, tasks, and models. Wongthongtham et al. (2008) present software engineering ontology that captures software engineering knowledge and enhances the sharing of this knowledge in various geographically disperse software development environment. Niculescu & Rrausan-Matu (2009) present competence management system (CMS) ontology in support of systematic knowledge acquisition regarding the competence of project members in their project management activities.

Furthermore, Van Ruijven (2013) presents a system information model that represents the ISO 15288 system engineering process for better interpretation in performing project development activities. Falbo et al. (2003) present ODE ontology discusses the environment and resources in the software development activities in the software lifecycle process. Henderson-Sellers et al. (2014) present CDO ontology that discusses relevant concepts in a particular environment of standards and working groups in project management. Rocha (2018) presents DKDOonto ontology for distributed software development process in support of better communication among the project team members with common and shared vocabulary. Gharib et al., (2020) present COPri ontology that discusses the privacy requirements in collecting, storing, and processing personal information. Kitchenham et al. (1999) present a system maintenance ontology that also describes various private confidential and public open access data. Also, discuss corrective and adaptive maintenance work in the system

operation. And change control process of evaluating the changes requests to approve or disapprove the system modification request. Ruiz et al. (2004) present software project maintenance ontology discusses the dynamic issues related to the management of maintenance related activities and tasks in various projects of software and information system development.

Furthermore, Yanuarifiani et al. (2020) present rule-based ontology in support of the requirements elicitation process while avoiding the possibility of missing or mismatching the requirements in preparing the requirements specification documents. Hallberg et al. (2014) present system development ontology that discusses the fundamental definitions of general concepts, description concepts, realization concepts, and appearance concepts, also their dependencies and relationships in the systems development activities. Bastos et al. (2018) present SPM ontology in support of software project management activities related to time, cost, and scope management. Hughes (2010) presents project management process ontology that describes the project management procedures prescribed by the Project IN Controlled Environment (PRINCE). Sheeba, et al. (2012) present a project management knowledge ontology that describes the artifacts and human resources to be used in the activities regarding the project management body of knowledge (PMBOK) aiming to support distributed system development activities. Wibowo & Davis (2020) present requirement traceability ontology in support of tracing requirements in the agile software development process. Annamalai et al. (2011) and Bianchini et al. (2006) present e-service ontology that discusses various classifications of electronic services according to branches and its processes. Lemey & Poels (2011) present service system ontology discusses the mapping of fundamental service system concepts on the service theories and frameworks in service science domain. Yustianto et al. (2018) present SoaML service ontology that defines the relationships between various related components regarding service engineering context in business management and information system development environment. Al-Sayed et al. (2020) present CloudFNF Ontology discusses various relations in the functional and non-functional properties of the cloud e-services.

Finally, it can be summarized from the above literature review that the proposed ontologies, methods, and techniques are primarily focused on extracting the regulatory rules, requirements, system components, services from various policy and regulation documents, and also from the system development activities and practices. However, how a legislation may or may not affect the E-Government and information system development projects is often not easily identifiable due to lack of clear understanding of the regulatory requirements compliance as well as the domain gap between E-Government, legal sciences, and IT systems development. Therefore, this study fills the research gap by incorporating the regulations, E-government, and information system development domain together through the use of EGRRC ontology and CISMET ontologies.

1.6 Research Contributions

The literature studies presented in section 1.5 have discussed various ontologies and methods in E-Government, policy and regulations, and IT system development domain. Such as in E-Government domain ontologies and methods are presented in E-Government project management and monitoring, E-Government web content analysis, E-Government service structure and their interoperability issues, E-Government service goal and their quality evaluation, E-Government privacy, and security requirements, etc. In the legal domain methods and techniques are presented in extracting and organizing the regulatory rules from various policy and regulation documents. Furthermore, in IT systems development domain ontologies and methods are presented in describing various process, activities, actors, objectives, and properties of system development lifecycle.

However, the intersection of these three domains: legal, government-administrative, and IT development remains a painstaking task and difficult to communicate due to the difference in terms, culture, analysis, cascading requirements, and the interconnection of concepts belonging to different domains. Hence, a comprehensive ontology would become a powerful instrument to integrate the key concepts of E-Government, policy and regulations, and information system development thus bridging the existing gaps between these three domains. Therefore, the main contribution of this research is to introduce the EGRRC and CISMET ontology frameworks and discuss the implementation of the ontology in the recently enacted General Data Protection Regulation (GDPR) for personal data processing in EU member countries. Thus, bridging the legal, government-administrative, and IT systems development domain together in order to assist in the detection of compliance related tasks and actions needed in parts of the regulatory compliant E-Government information system development project.

The E-Government researcher and practitioner can use the EGRRC ontology framework as a guideline to clearly understand the source, objective, and effects of the regulations and regulatory requirements in various types of E-Government services. Also, the system developer can define the priorities and potential amendments of various types of regulatory requirements extracted from regulatory rules in the E-Government service development from a regulatory perspective. Moreover, the EGRRC ontology framework will provide an opportunity to the E-Government system developer to implement existing legislations onto the EGRRC ontology that will allow them to make various queries about the effects of the legislation in the E-Government services development. For example:

- What are the regulatory documents that have an agreement with the data owners of the systems or third-party service providers in developing E-Government systems and how long the agreement will be valid?

- What regulatory requirements have long-term abstract or short-term immediate goals in developing the E-Government system? What E-Government services are affected by the regulation?
- What regulatory requirements in the regulations specify the system development properties, functional properties, and quality properties of the E-Government system?
- What are the constraint rules enacted in the regulation that restrict the system operations? What rules from the regulation generate formulas to be used in the system operations?
- What regulatory rules have high priority requirements that made obligatory in the E-Government system development? What rules are optional that the developer can implement in the E-Government system but not required to?
- In what part of the regulatory requirements may have amendments possibilities for further modification in the E-Government systems?

Furthermore, implementation of the regulations in EGRRC ontology will suggest the system developer with not only explicit regulatory requirements but also extract the implicit relations among various concepts used in regulatory requirements compliance of E-Government system development. This capability will be particularly helpful for the E-Government system analyst to clearly understand and define the implicit relations and constraints besides the explicit knowledge of the regulatory requirements in the regulation that the system developer might not have thought of otherwise. And the visualization of the explicit relations with what is implicit will certainly improve in the process for better compliance management of regulatory requirements in E-Government system development.

Moreover, the EGRRC ontology framework has been linked with the CISMET ontology which presents the technical concepts of information system development. So that, the guidance to the E-Government system developers also includes the guidelines around technical modifications that need to be performed for the IT systems to adapt to newly introduced legislative actions such as GDPR that affect them. Some typical examples of these queries that the project team asks for a successful project development are derived from IT project management practices (Olson, 2020; Hartley, 2018; Pressman, 2014) and existing ontologies in information system development (Table 5) are included here, but are not limited to:

- What are the system development goals referenced in the regulations (e.g., GDPR) to be implemented? And who are in control of pursuing the fulfillment of these system development goals?
- What activities/tasks are referenced in the regulation that describe the system development process?
- What system tasks may enhance the system functionality but not required? And, what tasks become obliged by regulation to perform in the system operation?
- What system services are affected by the regulations?

- What are the regulatory requirements for Data or Authentication Services referenced in the regulation?
- Which service needs private data in its operations? Who are the authorized system users to access those services?
- What roles are responsible to provide services to the system users?
- What tasks are referenced in the regulation that describes the system development process?
- What system activities/tasks referenced in the regulation are permissible and/or restricted to be performed in the system/project operations?
- What are the project development activities referenced in the regulation?
- What are the triggering events or task in performing the system activities?
- What constraints are placed by the regulations in performing the system activities/tasks?
- What resources are referenced in the regulation to be used in system development? What application/tools and hardware are imposed to be used in the system operation?

The General Data Protection Regulation (GDPR) is implemented in the EGRRC and CISMET ontology to demonstrate the results of the above-mentioned queries. The newly formed GDPR regulation enacted on 25 May 2018 that constitutes the legal framework for personal data processing all over the European member countries and the external organizations that are operating in the EU zones should comply with the regulation. The GDPR compliance should be the key priority to the local and central governments of EU countries who process personal information to avoid costly penalties of up to €20 million for non-compliance. The GDPR regulation has been implemented in this study by instantiation of the concepts regarding personal data processing found in the GDPR regulation and mapping these concepts into the entities of the EGRRC and CISMET ontology.

Nonetheless, some other regulations such as the regulations listed in Table1 can also be implemented in the EGRRC and CISMET ontology to demonstrate the ontology query results based on that regulations. The regulation document (e.g., HIPPA, SOX, ISO/IEC Security standards, etc.) texts can be used and mapped in populating the instances of the defined ontology classes and create the ontology framework descriptions. And relevant queries can be demonstrated to present the results of the queries that can aid the involved stakeholders to understand how the implemented legislation affects them and what actions are needed from their side as part of their positioning in the system development process.

Moreover, a major concern regarding the E-Government system development in today's world is to enhance the interoperability of E-Government operations and its service delivery. The goal of achieving the interoperability in E-Government operation is to exchange data or services through collaborating with various public and private organizations to provide one-stop E-Government services to the users

(Kalogirou et al., 2019; Nakakawa & Namagembe, 2019; Othman & Razali, 2017). The most critical issue regarding implementing interoperable E-Government system development is the integration of new technology such as blockchain and G-Cloud for transforming the public administrations that facilitate information flow between government agencies, private organizations, and citizens in a highly regulated area. In particular, the E-Government system development should be analyzed into multilateral issues such as technical, organizational, and legal aspect (Gerontas, 2020; Charalabidis et al., 2019). Therefore, the intersection of these three domains: legal, government-administrative, and IT development is a painstaking task due to the difference in terms, culture, analysis, cascading requirements, and the interconnection of concepts belonging to different domains. Hence, the EGRRC and CISMET ontologies become a powerful instrument to integrate the key concepts of E-Government, policy and regulations, and information system development thus demonstrates the bridging of existing gaps between these three domains (Figure 5).

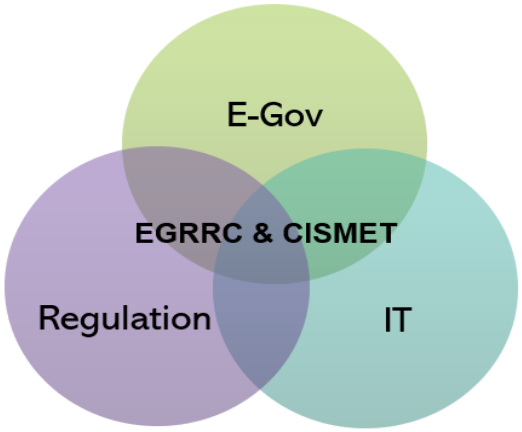


Figure 5: Bridging Legal, E-Gov, and IT domain

Furthermore, Layne & Lee (2001) define the E-Government system development initiatives into various levels where the implementation of E-Government in public sector is an evolutionary phenomenon (Figure 1). The integration of E-Government services among not only from different levels of government agencies (i.e., vertical integration) but also from different functions across government agencies (i.e., horizontal integration) has become the most highlighted concern towards the advancement of E-Government solutions. Here, the research questions of this study contribute to the vertical and horizontal level of E-Government evolution by providing a platform through the EGRRC and CISMET ontology to discuss various interrelated issues regarding the legal, government administration, and IT systems development. The first research question integrates the concepts of policies and regulations in E-Government domain through EGRRC ontology thus bridging these two domains. And the second research question integrates the concepts of E-Government regulatory requirements compliance (EGRRC ontology) to the compliant information system development project (CISMET), thus bridging the legal, government-administrative, and IT systems development domain together in order to

assist in the detection of compliance related actions needed in parts of the E-Government system development project. For example, annotating the system/software components or services with the concepts from EGRRC and CISMET ontologies (e.g., regulatory rules, requirements, services, goals, activities, resources, artifacts, etc.). This way, when a developer includes a component or service in their system/software application, the requirements stemming or inferred from this concept can be automatically detected and communicated to the developer of an actual software implementation.

1.7 Thesis Organization

Figure 6 shows the organization of this thesis work into primary milestones and correspondent chapters. The research background information regarding the E-Government regulatory requirements compliance has been discussed in section 1.1 and 1.2 (Chapter 1). Furthermore, the problem statements and research motivation (i.e., what is the problem and why this problem is very significant and has severe consequences in the research and practitioner community?) have been explained in section 1.3 (Chapter 1). Hence, the research objectives with research questions have been discussed in section 1.4. Furthermore, a state-of-the-art of existing works in the research domain has been presented in section 1.5 (Chapter 1) to understand and map the research contributions of this thesis along with the existing research activities in the domain. And the research contribution of the thesis works has been discussed in section 1.6 (Chapter 1).

The adopted research methodology, the Design Science Research Methodology (DSRM) and Systematic Literature Review (SLR) followed the step-by-step process of the solution design has been explained in Chapter 2. The development of the proposed solution, E-Government Regulatory Requirements Compliance (EGRRC) ontology framework has been explained in between sections 3.1 to 3.5 (Chapter 3). The proposed EGRRC solution has been demonstrated in section 3.6 (Chapter 3) through serving various E-Government service development queries by implementing the General Data Protection Regulation (GDPR) enacted in the European Union (EU).

Furthermore, in Chapter 4, the proposed solution has also been demonstrated by integrating the EGRRC ontology with the regulatory Compliant Information System developMEnT (CISMET) ontology extracted by reviewing the existing ontologies presented in the information system development domain which answers various IT system development queries based on the newly enacted GDPR regulation. Moreover, in section 4.6 (Chapter 4), a relevant software application has been developed, that aims to demonstrate the guidance of the IT system developer towards serving results of various queries regarding the modifications around technical aspects of the IT system development while adapting the legislative actions on the system components.

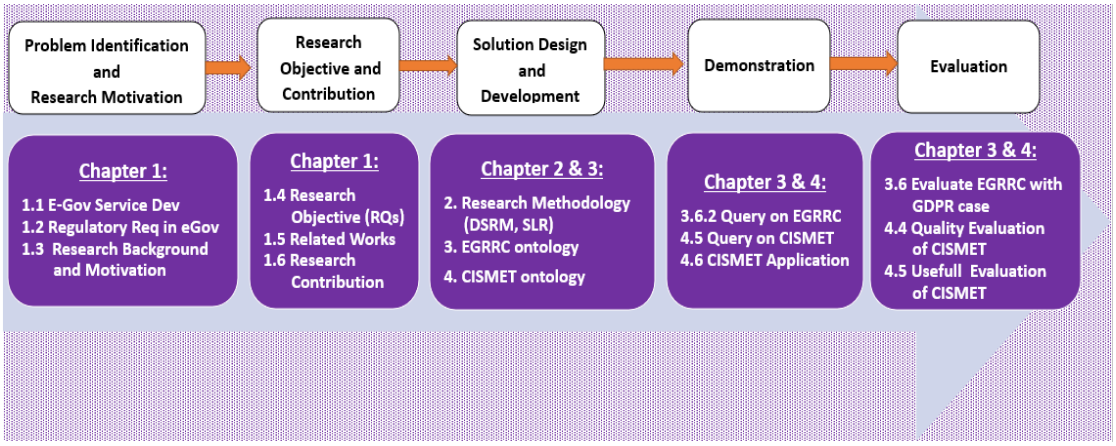


Figure 6: Organization of the Thesis works

The evaluation process (i.e., Quality Evaluation and Usefulness evaluation) of the EGRRC ontology has been described in section 3.6 (Chapter 3) and the evaluation of CISMET ontology has been described in sections 4.5 & 4.6 (Chapter 4). Section 5.1 discusses the summary of the research works such as existing challenges in research/practice in the field of E-Government system development and contribution of the research works with its innovation and evolution process. Section 5.1 also discusses the design rationale that presents the research decisions taken in this thesis. Finally, section 5.2 discusses the limitations address by this study and related recommendations for the future works.

Chapter 2: Research Methodology

The Design Science Research Methodology (DSRM) is generally adopted to conduct this research. DSRM is used in this study as a research paradigm in which the EGRRC and CISMET ontology frameworks have been introduced and evaluated for the problems of regulatory requirements compliance in E-Government system development. DSRM has been adopted and evaluated in several Information System research that provides a nominal process model for doing research and also provides a mental model for presenting and evaluating solutions of the research (Hevner & Chatterjee, 2010; Peffers et al., 2007; Peffers et al., 2006).

In the DSRM process, there are six systematic steps (Figure 7) to be followed to conduct scientific research. Firstly, the motivation of the research has been described with a significant need for a framework that describes the concepts of regulatory requirements and their interrelations in E-Government system development. The motivation of this study is drawn as a consequence of the problems on a very high risk of non-compliance with the regulatory requirements in information system development particularly in the E-Government system development because of a research gap for a comprehensive framework that describes the regulatory requirements in E-Government system development. And the system analysts have been facing many uncertainties and unanswered questions while handling with regulatory requirements compliance issues of the E-Government system development. As a result, the objective of this study is to introduce the E-Government Regulatory Requirements Compliance framework (EGRRC) and Compliant Information System developMEnT (CISMET) ontology framework that describes the interrelated concepts of regulatory requirements compliance and answers the queries of the system analyst regarding compliance of regulatory requirements in their E-Government system development projects.

The Systematic Literature Review (SLR) technique is used in the DSRM design and development process to review, analyze, reuse, and extend the available concepts of regulatory requirements compliance in introducing the EGRRC ontology framework from existing ontologies and general published literature in the domain of E-Government, information system development and regulations based on the ontology engineering guidelines. In order to show the research development and obtain a deeper understanding of a research field, the literature review is the most useful method that reviews various research papers, articles, and books presented in the research area. In fact, it is the most appropriate research method to meet as many experts and researchers in the research area with their various views and opinions as one can possibly do (Gunda, 2008).

A complete and successful literature review depends on the relevant literature selection, analysis, and presents the findings in a clear and coherent manner. Webster

& Watson's (2002) literature review guidelines and Gronlund & Andersson's (2006) literature selection and analysis guidelines were adopted in this research. The selection and analysis of the literature were based on the reliability, relevance, timeliness, and reputation of the literature. Major attention was given in the high ranked leading journals and conference proceedings that have a very high reputation for the quality of literature. Nonetheless, Webster & Watson (2002) argues that a complete and successful literature review not only considers the reputed journals and conferences, but also some other relevant sources of literature as well. Therefore, other relevant journals and conference proceedings were also explored in order to maximize the range of literature review.

A comprehensive review model is the prerequisite of a literature review in order to specify and validate the review process of literature search, selection, and analysis within a bounded research area (Webster & Watson, 2002). Figures 8 and 9 show the systematic way of literature search and selection procedure of the literature review model. Within a specific research topic, the review model guides literature search in the databases (e.g., journals and conference proceedings) applying search criteria of selected keywords, time frame, search area (e.g., title, abstract), and research field (e.g., E-Government, information system, regulations). The selection and sorting of the literature are based on the contribution relevant to the research topic of regulatory requirement compliance of E-Government and information system development.

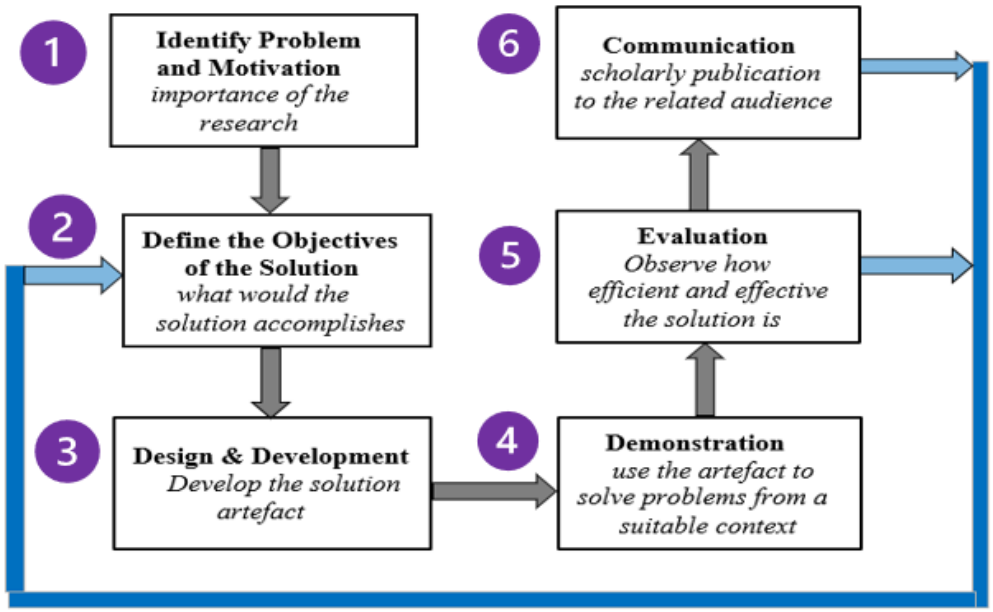


Figure 7: Design Science Research approach

In the demonstration phase of the DSRM process, a case study is conducted on the General Data Protection Regulation (GDPR) implementing the EGRRC ontology framework to demonstrate the use of the EGRRC ontology in answering the queries of the system analyst regarding regulatory requirements compliance in E-Government

system development. Next, the proposed EGRRC ontology is evaluated against the systematic evaluation criteria that ascertain the consistency, completeness, conciseness, clarity, generality, and robustness of the concepts and their relationships in the proposed EGRRC ontology framework. Also, the usefulness assessment of the proposed EGRRC ontology has been validated that meets the defined research objectives of understanding the compliance of the regulatory requirements in E-Government system development and provides correct and expected answers to the system analyst's queries regarding the compliance of the regulatory requirements in E-Government system development.

Finally, the research outcome is communicated to the E-Government practitioner and researcher through journal and conference publications. It communicates the existing problems of non-compliance and lack of studies on regulatory requirements compliance in E-Government system development. The necessity and importance of a framework describing the interconnected concepts of regulatory requirements compliance in E-Government system development. The novelty and usefulness of the new solution as well as the rigor of the design and development of the EGRRC ontology framework has been discussed. Also, the effectiveness of the EGRRC and CISMET ontology to the E-Government practitioner in designing a regulatory compliant E-Government system and to the researcher for future research scope in the area of E-Government system development.

2.1 Systematic Literature Review (SLR)

Systematic literature review (SLR) is used in this study to investigate the concepts of regulatory requirements compliance from existing ontologies and general literature presented in the E-Government domain to propose the EGRRC ontology framework. The SLR process can be one of the two types, conventional SLR aggregates results related to a specific research question to provide statistical results and analysis while mapping SLR finds and classifies the primary studies in a specific research topic. This study falls into the mapping category of SLR and follows the systematic steps (Figure 8) suggested by Kitchenham et al. (2010) and Petersen et al. (2008). Mapping SLR is the most appropriate choice to meet the objective of this research because this study undertakes a conceptual analysis of various issues regarding E-Government regulatory requirements compliance presented in the literature where conventional SLR provides only the quantitative comparisons of statistical data analysis.

Figure 8: Systematic Literature Review (SLR)

2.2 Literature Search Strategy

Eight databases known for reputed journals and conference proceedings in information system domain (SpringerLink, IEEE Xplore, Science Direct, Emerald Insight, Taylor & Francis, IGI Global, Wiley, and ACM online library) have been explored in the literature search process. Nonetheless, Webster & Watson (2002) argues that a complete and successful literature review considers all sources of literature rather than concentrate only reputed journals and conferences. Hence, Google Scholar that includes all the underlying libraries was also employed in the search process to find any missing literature in the database search and also explore any other sources of literature for relevant ontologies and literatures regarding the research topic. Google Scholar scans everything on the internet and nearly finds all the research works. This is particularly useful in adapting the concepts of Linked Data paradigm to reuse, extend, and combine existing ontology concepts while avoiding any duplication of the information (Polleres et al., 2020; Kalampokis et al., 2019).

Keyword selection for the literature search has significant importance in literature review process. A wide range of keywords have been used in the title, keywords, and abstract of the published literature, for example:

- (“E-Government” OR “Digital Government” OR “Public Service”) AND (“Regulation” OR “Policy” OR “Legal” OR “Law” OR “Regulatory Requirement”) AND (“Compliance”) AND (“Ontology” OR “Semantics”)
- (“Information System” OR “IT System” OR “Software System” OR “Software Process” OR “Software Engineering” OR “System Engineering”) AND (“Ontology” OR “Semantics”)
- Information System Development” OR “IT System Development” OR “Software System Development”) AND (“Ontology” OR “Semantics”)
- (“Information System Project” OR “IT Project” OR “Software Project” OR “Project Management”) AND (“Ontology” OR “Semantics”)
- (“System Service” OR “Service Development” OR “System Development”) AND (“Ontology” OR “Semantics”)

To ensure not to miss out the relevant literature, the synonyms of the keywords or the phrases that might describe the concepts of the keywords have also been used in the search process. Furthermore, various combinations of keywords in the search statements have also been formulated using AND, OR Boolean operators as suggested in Web of Science. The literature search was conducted until August 2020 and there was no time frame limitation for the publication year in the literature search, i.e., literature published in any year were set to be searched. Furthermore, backward, and forward search were also used in the search process as suggested in Web of Science where backward search reviews the relevant reference list of the literature and forward search reviews the literature that cites the identified literature. Also, the

citation index of the selected paper's author was also reviewed from DBLP to find the relevant literature from their publication citation lists.

2.3 Literature Selection Criteria

The inclusion and exclusion criteria of literature search and selection sets the boundaries of the systematic literature review process. For the analysis, the literature was included only if the literature is written in English and the abstract of the literature explicitly mentions the concepts of regulatory requirements compliance, E-Government, information systems, IT systems, or software systems development. From the search process, the literature was excluded if there are multiple publications exists on the same research scope by the same research group. In that case, the most complete publication was considered for further analysis. Moreover, the literature that presents the concepts other than regulatory requirements compliance, E-Government, and information system project development were excluded for data extraction. In other words, the literatures were excluded if they did not provide any information regarding the concepts of class definitions and class properties for the ontology of regulatory compliant E-Government and information system development projects.

2.4 Data Extraction and Analysis

In the initial screening process in the database, we looked into the literature that explicitly presents ontologies or semantics in the field of E-Government, policy and regulations, information systems, IT systems, or software systems development projects. A total of 269 literature were selected from the initial screening of the literature search placed in the title, abstract, and keywords of the published literature. There are 165 literature discuss the ontology classes and properties that do not directly related to the E-Government, regulation, and information system project development. For example, the ontologies and semantics are presented in the area of information retrieval/extraction/ collection/gathering, e-learning system, cybersecurity and logistics systems, healthcare/clinical/medical/biomedical/disease information systems, IoT based system and service, library management system, geographical/ location mapping system, etc. Moreover, while we were reviewing the author's citation index in DBLP, also applying backward and forward searching process in the database, we have found that there are 26 literature discuss ontology classes and properties in the literature that are taken from the part of the ontologies proposed earlier by the same research group. In this case only the literature that provides the complete class and property definitions were included for further analysis.

However, we were investigating a very specific topic of regulatory compliant E-Government information system development project with a very specific technology of implementation (OWL). Based on the inclusion and exclusion criteria discussed above, there are 78 literature address policy and regulations in the E-Government and

information system development as their primary contribution. Among the 78 literature, there are 24 literature propose ontologies in E-Government and regulation domain, 27 literature propose ontologies in information systems and 27 literature address policy and regulations in e-Government domain as their primary contribution. Hence, these 78 literature were finally selected for data extraction that provides the class definitions and properties in the regulatory requirements compliant E-Government information system development domain. The derived concepts of class hierarchy and relationships among them are presented in Table 2, 3, and 5. The derived concepts are then analyzed in describing the classes and properties of E-Government and Information system development and their relationship with the regulatory requirements compliance domain using the ontology development tool Protégé (Horridge et al.,2004).

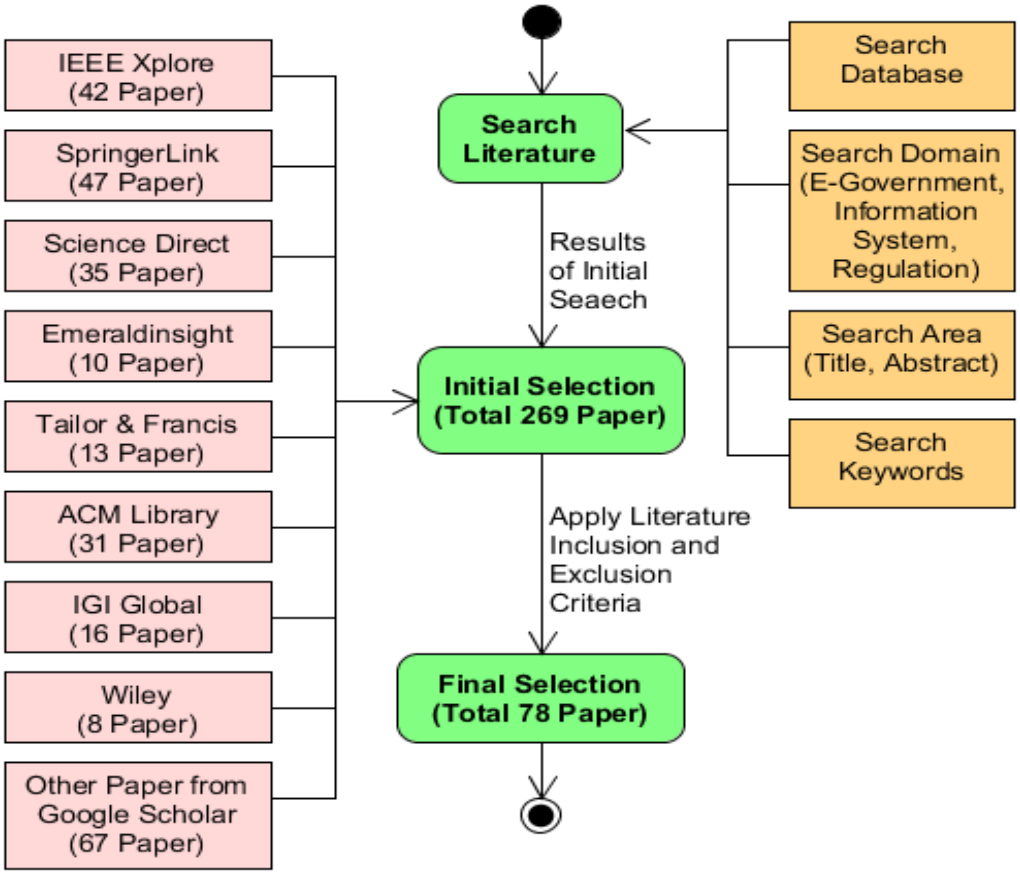


Figure 9: Findings of the Literature Review

The data was extracted in the following categories for understanding the regulatory requirement compliance in E-Government information system development. The sources of regulatory requirements in E-Government system development, objectives of the regulations, E-Government services affected by the regulations, types of regulatory requirements, formulation of rules in the regulatory requirements, priority of regulatory requirements, and changing nature of regulatory requirements in E-Government system development. The EGRRC ontology captures this knowledge

existing in the E-Government and regulation domain by describing the concepts and the relationships behold between those concepts. Furthermore, The CISMET ontology captures the knowledge of system development goals, services, process, activities, and resources used in the information system development projects.

Ontology presents the existing unstructured data in a domain into structured information that describes the formal and explicit specification of conceptual information, and their relations exits in some specific domain (Khadraoui et al., 2005). Ontology engineering is still in its infancy and does not have a process model that is as much popular and accepted as a standard as that we can find in the software engineering domain. Different researcher and practitioner groups have proposed their own ways and methodologies of building ontologies which greatly depend on the size, nature, and application of the domain where ontology is being built. However, the consideration has been given in this research to find the state-of-the-art knowledge and rules on ontology engineering methodologies based on the guideline "Ontology Development 101" that is more practical with logical and ethical values (Noy & McGuinness, 2001). Furthermore, the extracted data from the systematic literature review are analyzed to be reused and extended in the development of the EGRRC ontology framework. And the implementation of General Data Protection Regulation (GDPR) into the defined entities of EGRRC ontology has been demonstrated using Protégé tool based on the systematic guideline provided by "A Practical Guide to Building OWL Ontology using Protégé" (Horridge et al., 2004).

Step 1: Determine the Domain and Scope of Ontology

The starting point of each ontology development is to define the domain and scope of the ontology. The EGRRC ontology development defines the scope of the regulatory requirements compliance in the E-Government system development domain. The EGRRC ontology framework is introduced to the E-Government system developer as a comprehensive guideline to clearly understand the impacts of regulatory requirements compliance in the E-Government system development. Also, the EGRRC answers various queries of the E-Government system analyst in identifying the source, objective, effects, and priorities of different types of regulatory requirements from various regulations.

Step 2: Consider Reusing Existing Ontology

In ontology development, it is worth considering some of the existing ontologies in the fields. It is often supportive in the ontology development process to refine, reuse, and extend some of the already existed concepts in the ontology. The systematic literature review is used in the EGRRC and CISMET ontology design and development process to review, capture, analyze, reuse, and extend the available concepts of regulatory requirements compliance in the process of E-Government and Information system development (Table 2 &3 and Table 5).

Step 3: Create Class and Class Hierarchy

The classes are the main building blocks of building ontologies. There are multiple possible approaches in developing a class hierarchy of concepts. The top-down approach starts with defining the most general concepts of classes in the domain first and then subsequent specialization of the concepts, the bottom-up approach works in the other way of defining the most specific classes first and then a subsequent grouping of these class into more general concepts, a combination approach starts with defining the most noticeable concepts first and then generalize and specialize them appropriately. In EGRRC ontology, the classes describe the existing and extended concepts in the E-Government domain in a top-down approach where the classes can have multiple subclasses that represent the more specific concepts of superclass. The EGRRContology class hierarchy describes the collection of classes where the specific purpose subclasses are described under the general purpose of superclass (Figure 17-19).

Step 4: Create Class Properties

The classes alone will not provide sufficient information to understand a domain area. Once the classes are defined in an ontology then it is necessary to describe the structure of the class through describing the properties of the classes that represent the relationships between the classes in the ontology. In EGRRC ontology, the class properties are extracted, reused, and extended from existing ontologies and general published literature in the E-Government domain in making relationships between the classes in the class hierarchy in describing the information presented in the EGRRC ontology (Figure 20-28). In describing the EGRRC classes and class properties, the subclasses by default inherit the properties defined in its superclass.

Step 5: Create Individual instances

The final task of ontology engineering is to create individual instances or objects of classes in the class hierarchy. Individual instances are the most specific concepts represented by the classes of a knowledge area. The EGRRC ontology classes have been instantiated with the instances found in the General Data Protection Regulation (GDPR) regarding personal data processing across the organization under the European Union (EU) zone. The mapping of individual instances into the EGRRC ontology classes may help the E-Government system developer in EU countries to understand the most precise information on how the newly introduced GDPR legislation affects in the E-Government system development.

Chapter 3: EGRRC Ontology Framework

The results of the systematic literature review (SLR) are presented here in Table 2 and Table 3. The elements of the EGRRC ontology are extracted by reviewing the existing ontologies as well as general published literature presented in the E-Government and legal domain. Specifically, for the reuse of the existing ontologies, this is based on the spirit of the Linked Data paradigm (Polleres et al., 2020; Kalampokis et al., 2019, Färbe et al., 2018; Bizer, 2009), an approach to cross-reference elements from existing ontological vocabularies in order to enhance the reusability and extension of the existing concepts.

3.1 Existing Ontologies in E-Government Domain

The following table illustrates the elements of the EGRRC ontology. In each table entry, the 'Ontology' field provides the name and references of the existing ontologies in the information E-Government and regulatory requirements domain and the 'Main Focus' field presents the primary contributions of the ontologies. The 'Class Hierarchy' field presents the hierarchy of classes extracted from existing ontology descriptions, the 'Class Property' field presents the interrelations between the classes, the 'Triple' field presents the relationships among the subject class and object class through class properties. It also presents the origins of the classes and properties (from which ontologies are imported/extracted). The subject class, object class, and the class properties (i.e., predicates) in the triple are leveled with alphabetical order. For example, the subject class level with 'a' has a relationship with the object class level with 'a' through the class property level with 'a'.

Table 2: EGRRC Ontology Elements derived from Existing Ontologies.

ONTOLOGY Name	**E-Government Project Monitoring Ontology (Dombeu, 2010); OntoAL (Shehu & Xhina, 2019); Semantic Government Process Management (SGPM) ontology (Cherouana et al., 2019)**
Ontology Main Focus	The ontologies describe various types of roles in the E-Government project development. The financers are government and non-profit organizations who financially support from their different level of section and subsection in the E-Government projects. The supplier, contractor, and consultant are involved in the project as a private organization who provides support to the project development. And project manager and developer are the team members of the project who carried out the project development task.
Class Hierarchy and Class	**Classes Hierarchy:** • *Superclass:* e-Gov Donor [Subclass: Directorate, Division, Unit] • *Superclass:* Service Provider [Subclass: IT Service Provider]

Properties derived from the ontology	**Class Properties**: • hasFund class property makes relationships between E-Gov Donor class of Stakeholder with the E-Gov Service class and Percentage class of rule components to define who funds (e.g., Directorate, Division, or Units of Government organization and NGO) of what percentages (e.g., 80%, 50%) in the E-Government Service development. • hasProvideTechnicalSupportTo class property describes the relationship between Service Provider (i.e., IT vendors) class with the E-Government Service class where the supplier, contractor, and project members are supporting in the development of E-Government system. **Ontology Triple:** *Subject Class:* E-Gov Donor (a), Service Provider (b) (origin: E-Gov Project Monitoring ontology, OntoAL ontology, SGPM ontology) *Class Property:* hasFund (a), hasProvideTechnicalSupportTo (b) (origin: EGRRC ontology) *Object Class:* Percentage (a), E-Gov Service (b) (origin: EGRRC ontology (a), SGPM ontology (b))
ONTOLOGY Name	**OntoAL ontology (Shehu & Xhina, 2019); SGPM ontology (Cherouana et al., 2019); Web Content (WC) ontology (Thomas & Elnagar, 2018)**
Ontology Main Focus	The SGPM and WC ontologies describe the laws and regulations for the public services. The OntoAL ontology describes governing e-services structures in the Albanian E-Government system development. And provide feasible and meaningful E-Government services to the Albanian citizens based on the regulations. Furthermore, the ontology also could be helpful in the process of introducing and modifying e-services in the mission of the e-Albania movement.
Class Hierarchy and Class Properties derived from the ontology	**Classes Hierarchy:** Superclass: Regulatory Source [Subclass: Legal Document] **Class Properties**: • hasAuthoritativeRegulationOf class property describes the relationships between Legal Document class with the E-Gov Service class as the legal document has the national and even wider level authority (e.g., EU) to describe the E-Government services such as Federal regulation, GDPR. And often the public e-services development is primarily based on the laws enacted by the government. **Ontology Triple:** *Subject Class:* Legal Document (origin: OntoAL ontology, SGPM

	ontology, WC ontology) *Class Property:* hasAuthoritativeRegulationOf (origin: EGRRC ontology) *Object Class:* E-Gov Service (origin: SGPM ontology)
ONTOLOGY Name	**E-Government Project Management (eGPM) Ontology (Sarantis & Askounis, 2009); OntoAL (Shehu & Xhina, 2019)**
Ontology Main Focus	The ontologies describe the E-Government project knowledge into various fundamental concepts. The primary beneficiary of the E-Government systems who receives the E-Government services. The administration levels are the government structure who provides E-Government service to the service recipient. The domains are the areas of the government sector (e.g., education, agriculture, finance, etc.) where the E-Government system is to be performed in relation to provide E-Government services to the citizen, business organization or the government employees. The functions are the front office system interface from where the service recipients of the E-Government system are receiving e-services and back-office systems are working in the background of the interface where multiple systems are interoperating together to produce the E-Government service. And, the project nature defines the more precise information of the E-Government project to be used in other similar projects.
Class Hierarchy and Class Properties derived from the ontology	**Classes Hierarchy:** • *Superclass:* e-Gov Stakeholder [Subclass: E-Gov User] • *Superclass:* E-Gov User [Subclass: Citizen, Business Organization, Government Employee] **Class Properties**: • hasProvideServiceTo class property makes a relationship between the E-Government Service class with the E-Government Stakeholder class as various types of E-Government services provide their service to various types of stakeholders in the E-Government system. **Ontology Triple:** *Subject Class:* E-Gov Service (origin: E-Service ontology, OntoAL ontology) *Class Property:* hasProvideServiceTo (origin: EGRRC ontology) *Object Class:* Stakeholder (origin: E-Gov Goal ontology)
ONTOLOGY Name	**E-Gov Service Quality (e-GovQoS) Ontology (Corradini et al., 2006); Standardize Quality Service (SQS) ontology (Okike, 2017)**
Ontology Main Focus	The ontologies discuss various quality requirements in the E-Government systems. For example, Interoperability of the e-services provided by several public administrations increases the

	speed of service delivery and service accessibility to the citizens and business organizations. Thus, it increases the service integration competence of public administrations and reduces the cost of e-services towards user satisfaction.
Class Hierarchy and Class Properties derived from the ontology	**Classes Hierarchy:** • Superclass: System Requirements [Subclass: Quality Requirements] **Class Properties**: • hasQualityPropertyOf class property describes the relationships between the Quality Requirements class of the System Requirements with the e-Government Services class where the quality requirements describe the system's non-functional behaviour such as availability, performance interoperability, accessibility, security, accuracy, etc. **Ontology Triple:** *Subject Class:* Quality Requirements (origin: E-Government QoS ontology, SQS ontology) *Class Property:* hasQualityPropertyOf (origin: EGRRC ontology) *Object Class:* E-Gov Services (origin: EGRRC ontology)
ONTOLOGY Name	**E-Government System Quality (QeGS) ontology (Magoutas et al., 2007); Web Content (WC) ontology (Thomas & Elnagar, 2018); SQS ontology (Okike, 2017)**
Ontology Main Focus	The ontologies describe various E-Government system quality attributes. Furthermore, the ontologies are also proposed to assess the E-Government system quality from the citizens perspective as a user of the E-Government system services. The E-Government service quality such as usability, accuracy, accessibility of the E-Government information of the public website is assessed by achieving citizen's satisfaction and trust in information providing by the E-Government system.
Class Hierarchy and Class Properties derived from the ontology	**Classes Hierarchy:** • Superclass: System Requirements [Subclass: Quality Requirements] **Class Properties**: • isSourceOf class property describes the relationships between Regulatory Requirements with Regulatory Source class as various regulatory sources are the primary scope of the finding the regulatory requirements. For example, the External Regulatory Source (i.e., legal documents and standard documents) is primarily the source of Quality Requirements attributes of an E-Government system development.

	Ontology Triple: *Subject Class:* Regulatory Source (a) External Regulation (b) (origin: EGRRC ontology) *Class Property:* isSoruceOf (a, b) (origin: EGRRC ontology) *Object Class:* Regulatory Requirement (a) Quality Requirement (b) (origin: E-Gov Literature (a), E-Gov System Quality ontology (b), WC ontology (b), SQS ontology (b))
ONTOLOGY Name	**Compliance Management ontology (Stratigaki et al., 2016)**
Ontology Main Focus	The ontology discusses the process of eliciting various business processes from the regulatory documents in the real E-Government system development cases. And extract various compliance requirements from the E-Government regulatory documents and present in executable MTL pattern.
Class Hierarchy and Class Properties derived from the ontology	**Classes Hierarchy:** • Superclass: Rule Complexity [Subclass: Simple Rule, Compound Rule] • Superclass: Rule Component [Subclass: Restriction] **Class Properties**: • hasCoverage class property describes relationships between Compliance Probability class with the Rule Complexity class where a regulatory rule has Total Compliance when it covers all the conditions in a compound rule connected with a logical operator. On the other hand, the regulatory rule has Partial Compliance when it covers some parts of the Compound Rule. **Ontology Triple:** *Subject Class:* Compliance Probability (origin: EGRRC ontology) *Class Property:* hasCoverage (origin: EGRRC ontology) *Object Class:* Rule Complexity (origin: Compliance Mgt. ontology)
ONTOLOGY Name	**E-Government Goal (e-GovGoal) ontology (Salhofer et al., 2009); SGPM ontology (Cherouana et al., 2019)**
Ontology Main Focus	The ontologies discuss the goal of e-services provided by a public administration is to fulfill the needs of the service recipient based on the condition presented by the financier that produces the outcome of E-Government system such as effect and consequence of E-Government services.
Class Hierarchy and Class Properties	**Classes Hierarchy:** • Superclass: Stakeholder [Subclass: Service Provider] • Superclass: Service Provider [Subclass: Gov Agency] • Superclass: E-Gov Objective [Subclass: Regulatory Outcome]

derived from the ontology	**Class Properties**: • isGoalOf class property describes the relations between the Regulatory Outcome of Regulatory Objective class with the Internal Regulation class of the Regulatory Source (i.e., Regulatory Documents) class as the E-Government project outcome is often defined by various policies and agreements made in the E-Government project development based on the system requirements such as data backup policy. • hasProvideSupportTo class property describes the relation between Service Provider class with the E-Government Service class where the supplier, contractor, and project members are supporting in the process of E-Government information system development project. • hasProvideCollaborativeSupportTo class property describes relations between the Government Agency class of Service Provider with the E-Gov Service class where multiple public organizations are collaborating with each other to produce one-stop E-Government service. **Ontology Triple:** *Subject Class:* Regulatory Outcome (a), Service Provider (b) E-Gov Agency (c) (origin: E-Gov Goal ontology, SGPM ontology) *Class Property:* isGoalOf (a), hasProvideSupportTo (b), hasProvideCollaborativeSupportTo (b) (origin: EGRRC ontology) *Object Class:* Internal Regulation (a), E-Gov Service (b, c) (origin: EGRRC ontology (a), SGPM ontology (b, c))
ONTOLOGY Name	**Process and Compliance ontology (Schmidt et al., 2007)**
Ontology Main Focus	The Process and Compliance ontology describes the rules in the regulations are syntactic rule that defines the responsible role for each activity, semantic rule defines the actions and existence of certain structures in the service process, and pragmatic rule defines the abstract goal to be achieved by the service process in the long run of E-Government operation.
Class Hierarchy and Class Properties derived from the ontology	**Classes Hierarchy:** • Superclass: E-Gov Objective [Subclass: Regulatory Impact] **Class Properties**: • hasGoal class property describes the relationships between the Regulatory Source class with the Regulatory Objective class in describing the goals or objectives of E-Government service development from various sources of regulatory documents. • hasLongTermGoalOf class property describes the relationships between the Regulatory Impact class of the Regulatory Objective class with the Regulatory Requirements class in describing the abstract goals of e-service development to be achieved as the

	long-term benefits. Such as achieving citizen satisfaction on the E-Government system and building trust in the government. **Ontology Triple:** *Subject Class:* Regulatory Source (a), Regulatory Impact (b) (origin: EGRRC ontology (a), Process and Compliance ontology (b)) *Class Property:* hasGoal (a), hasLongTermGoalOf (b) (origin: EGRRC) *Object Class:* Regulatory Objective (a), Regulatory Requirements (b) (origin: E-Gov Literature)
ONTOLOGY Name	**E-Government Security ontology (Karyda et al., 2006); SGPM ontology (Cherouana et al., 2019)**
Ontology Main Focus	The E-Government Security ontology describes the security objectives of the case study of the e-Tax system are availability, confidentiality, security, accuracy etc. The countermeasures of security threats are access control, data backup policy, cryptography, firewall, certificates, introduction detection, security updates, etc.
Class Hierarchy and Class Properties derived from the ontology	**Classes Hierarchy:** • Superclass: System Requirement [Subclass: Quality Requirement] • Superclass: Regulatory Source [Subclass: Policy Document] • Superclass: E-Gov Objective [Subclass: Regulatory Outcome] **Class Properties**: • hasShortTermGoalOf describes the relationships between the Regulatory Outcome class of the Regulatory Objective class with the Regulatory Requirements class in describing the immediate goals of the e-service development. **Ontology Triple:** *Subject Class:* Regulatory Outcome (origin: e-Gov Security ontology, SGPM ontology) *Class Property:* hasShortTermGoalOf (origin: EGRRC ontology) *Object Class:* Regulatory Requirements (origin: E-Gov literature)
ONTOLOGY Name	**Core E-Government ontology (Amalanathan, 2015); SGPM ontology (Cherouana et al., 2019)**
Ontology Main Focus	The ontologies describe various roles in the E-Government system services. Furthermore, the ontologies also describe the E-Government system development using an evolutionary method where the core E-Government services are added to the system to extend the interoperability.
Class Hierarchy	**Classes Hierarchy:** • Superclass: E-Gov Service [Subclass: G2C, G2B, G2G]

and Class Properties derived from the ontology	**Class Properties**: • hasProvideServiceTo class property describes the relationships between various types of E-Government services (i.e., Government-to-Citizen, Government-to-Business, Government-to-Government) with the System users (i.e., Citizens, Business organizations, and Government employees) **Ontology Triple:** *Subject Class:* G2C (a), G2B (b), G2G (c) (origin: Core E-Gov ontology) *Class Property:* hasProvideServiceTo (a, b, c) (origin: EGRRC ontology) *Object Class:* Citizen (a), Business (a), Government Employee (origin: E-Gov Project Management ontology, SGPM ontology)
ONTOLOGY Name	**E-Gov Service Evolution ontology (Apostolou et al., 2005)**
Ontology Main Focus	The E-Government service evolution ontology describes the configuration of the E-Government service using ontologies because of the changes that may happen in the E-Government system development policy for ambiguous regulations. The implemented E-Government services and activities based on the legal premises may further be reconfigured as a result of changes made in the regulation.
Class Hierarchy and Class Properties derived from the ontology	**Classes Hierarchy:** • Superclass: Rule Status [Subclass: Dynamic Rule] **Class Properties**: • hasAmbiguityIn class property describes the relationships between Dynamic Rule class of Rule Status class with the Regulatory Rule class where the regulatory rules often change due to ambiguous descriptions in the rules. **Ontology Triple:** *Subject Class:* Dynamic Rule (origin: e-Gov Service Evolution ontology) *Class Property:* hasAmbiguityIn (origin: EGRRC ontology) *Object Class:* Regulatory Rule (origin: E-Government literature)
ONTOLOGY Name	**E-Government Service ontology (Stojanovic et al., 2004); Open Government Data Licenses Mash-up (OGDL4M) ontology (Mockus & Palmirani, 2017)**
Ontology Main Focus	The ontologies describe the E-Government services are referring to some law. And the ontology is used to find the corresponding changes in the E-Government system development if any changes take place in the service development policies. Also, the law

	enables us to find the corresponding service with possible action with pre-condition, post-condition, and any applicable restrictions that controls its execution.
Class Hierarchy and Class Properties derived from the ontology	**Classes Hierarchy:** • Superclass: Rule Component [Subclass: Task, Condition, Restriction] **Class Properties**: • hasAgreementValidity class property describes the relations between the Agreement Document class of Internal Regulations with the Restriction class of Rule Component as there are certain period is mentioned for every contractual agreement in the E-Government system development. **Ontology Triple:** *Subject Class:* Agreement Document (origin: E-Gov literature) *Class Property:* hasAgreementValidity (origin: EGRRC ontology) *Object Class:* Restriction (origin: e-Gov Service ontology, OGDL4M ontology)
ONTOLOGY Name	**E-Service ontology (Vassilakis & Lepouras, 2006); Web Content (WC) ontology (Thomas & Elnagar, 2018)**
Ontology Main Focus	The e-services offered by multiple government agencies are received by the citizen and enterprise based on the national official document and municipality practice who implements and regulates the operation of the services. The national regulations are perceived as a global view of regulation on the system operation that cannot be modified from the local government.
Class Hierarchy and Class Properties derived from the ontology	**Classes Hierarchy:** • Superclass: E-Gov Service [Subclass: Government-to-Citizen, Government-to-Business] • Superclass: Service Provider [Subclass: Gov Agency] • Superclass: E-Gov User [Subclass: Citizen, Business Organization] **Class Properties**: • hasAffect class property describes the relationships between Regulatory Source class with the Egov Service class as various regulations from different types of regulatory document has affects on the E-Government service development. • hasPropertyOf class property describes the relationships between Regulatory Requirements class with the E-Gov Services class where the regulatory requirements describe the project, system, functional, and non-functional characteristics of E-Government service development.

	Ontology Triple: *Subject Class:* Regulatory Source (a), Regulatory Requirement (b) (origin: EGRRC ontology (a), E-Government literature (b)) *Class Property:* hasAffect (a), hasPropertyOf (b) (origin: EGRRC) *Object Class:* E-Gov Service (a, b) (origin: E-Service ontology)
ONTOLOGY Name	**E-Gov Business Knowledge Modelling (EGBOnt) ontology (Xiao et al., 2007); OGDL4M ontology (Mockus & Palmirani, 2017)**
Ontology Main Focus	The ontologies describe that the E-Government task can be a sub-task of another task which represents the part-whole relationships between the tasks. Furthermore, the E-Government policy rules may affect in performing the E-Government task by linking corresponding constraints in system operations.
Class Hierarchy and Class Properties derived from the ontology	**Classes Hierarchy:** • Superclass: Rule Component [Subclass: Task, Restriction] **Class Properties**: • hasPerform class property describes the relationships between Regulatory Rule with the Task class of rule component as various types of regulatory rules (i.e., Action, Constraint, Computation) performs some tasks in the E-Government system operations. **Ontology Triple:** *Subject Class:* Regulatory Rule (origin: E-Government literature) *Class Property:* hasPerform (origin: EGRRC ontology) *Object Class:* Task (origin: E-Gov Business Knowledge Modelling ontology)
ONTOLOGY Name	**EGO ontology (Ortiz-Rodríguez & Villazón, 2006); SGPM ontology (Cherouana et al., 2019)**
Ontology Main Focus	The ontologies describe the information transaction in the e-service delivery process to the service recipient such as citizens and business organizations from various public administrative organizations. It also describes the large amount of information to be processed with transparency and efficient way by public administration to produce the E-Government service.
Class Hierarchy and Class Properties derived from the ontology	**Classes Hierarchy:** • Superclass: Stakeholder [Subclass: E-Gov User] • Superclass: E-Gov Service [Subclass: Government-to-Citizen, Government-to-Business] **Class Properties**: • hasProvideServiceTo class property makes a relationship between the E-Government Service class with the E-Government User class as various types of E-Government services provide e-services to the E-Government user groups such as citizens and

	business organization. • hasReceive class property describes the relations between the E-Government User class of Stakeholder with the E-Government Service class as various types of E-Government users receive various types of E-Government service. **Ontology Triple:** *Subject Class:* E-Gov Service (a), E-Gov User (b) (origin: EGO ontology, SGPM ontology) *Class Property:* hasProvideServiceTo (a), hasReveive (b) (origin: EGRRC ontology) *Object Class:* E-Gov User (a), E-Gov Service (b) (origin: EGO ontology, SGPM ontology)
ONTOLOGY Name	**Legislative ontology (Costilla et al., 2005)**
Ontology Main Focus	Legislative ontology explains that there is motivation behind every legislation which has a number of articles, chapters, sections, and rules. This is helpful to find the exact change location for insert, delete, and modify rules in the legislation document for any future scope of amendments.
Class Hierarchy and Class Properties derived from the ontology	**Classes Hierarchy:** • Superclass: Rule Status [Subclass: Dynamic Rule] **Class Properties**: • isOriginatedFrom class property describes the relationships between Dynamic Rule class with the Internal Regulation class (i.e., policy and agreement document) as the scope of changes may happen very often while making amendments in the policies and agreement of the E-Government system development. **Ontology Triple:** *Subject Class:* Dynamic Rule (origin: Legislative ontology) *Class Property:* isOriginatedFrom (origin: EGRRC ontology) *Object Class:* Policy Document (origin: E-Government Service Evolution ontology)
ONTOLOGY Name	**Policy domain language ontology (Barrett et al., 2007); OGDL4M ontology (Mockus & Palmirani, 2017)**
Ontology Main Focus	The ontologies describe the semantics of policy representation formats in the policy transformation process. Furthermore, the ontology describes that the policy condition determines the action to be executed. The policy actions are tested by a single condition or a set of conditions and restrictions.
Class	**Classes Hierarchy:** • Superclass: Regulatory Source [Subclass: Policy Document]

Hierarchy and Class Properties derived from the ontology	• Superclass: Rule Complexity [Subclass: Simple Rule, Compound Rule] • Superclass: Rule Component [Subclass: Task, Condition, Logical Operator, Restriction] **Class Properties**: • hasCoverWholeOf and hasCoverPartOf class properties describe the class relationships between Total Compliance and Partial Compliance classes with the Simple and Compound rules as the regulatory rules may cover the whole of a simple rule or part of a compound rule defined in the E-Government system development. **Ontology Triple:** *Subject Class:* Total Compliance (a), Partial Compliance (b) (origin: Policy domain language ontology) *Class Property:* hasCoverWholeOf (a) hasCoverPartOf (b) (origin: Policy domain ontology) *Object Class:* Simple Rule (a, b), Compound Rule (b) (origin: Compliance Management ontology, OGDL4M ontology)
ONTOLOGY Name	**Genpol policy wizard ontology (Campbell, 2006)**
Ontology Main Focus	The Genpol policy wizard ontology describes various trigger events such as GREATER THAN, LESS THAN, IN, AT in the regulatory rules to place restrictions on the conditional rule. It also describes various logical operators such as AND, OR, NOT, ELSE in policy rules to combine multiple conditions in a single regulatory rule.
Class Hierarchy and Class Properties derived from the ontology	**Classes Hierarchy:** • Superclass: Rule Component [Subclass: Logical Operator, Condition, Restriction] • Superclass: Rule Complexity [Subclass: Simple Rule, Compound Rule] **Class Properties**: • hasNumberOf class property describes the relationships between Rule Complexity class with the Logical Operator class of Rule Component where the rules may or may not have any logical operator in the formulation of the rules with various conditions. • isBasedOn class property describes the relationships between Simple and Compound Rule class of Rule Complexity with the Logical Operator class of Rule Component where the rule complexity (simple rule or complex rule) is decided by the number of logical operators used in the rule's formulation. **Ontology Triple:** *Subject Class:* Rule Complexity (a), Simple/Compound Rule (b) (origin: Compliance Management ontology)

	Class Property: hasNumberOf (a), isBasedOn (b) (origin: EGRRC) *Object Class:* Logical Operator (a, b) (origin: Genpol policy wizard ontology)
ONTOLOGY Name	**Generic Regulation Ontology (El-Kharbili and Stolarski, 2009); OGDL4M ontology (Mockus &Palmirani, 2017)**
Ontology Main Focus	The ontologies describe the modalities of the agreement such as Obligation where an actor must do some action, Permission where an actor can do some action, and Prohibition where an actor cannot do some action. The ontology also describes that the policy also specifies conditions using time, place, and context. The violation of policy rules also discussed in violation level and remedial action.
Class Hierarchy and Class Properties derived from the ontology	**Classes Hierarchy:** • Superclass: Regulatory Source [Subclass: Policy Document] • Superclass: Regulatory Authority [Subclass: Obligation, Privilege] **Class Properties**: • hasOrgRegulationOf class property describes relationships between Policy Document class of regulatory source with the E-Government Service class. The policy document presents the organization's own policies regarding a system development constraint where the E-Government system is being developed. • hasHardSatisfactionOf class property describes the relations between the Obligation class of Regulatory Authority with the Regulatory Requirement class as it requires completely 100 percent compliance of the regulatory requirement in the E-Government system development. • hasSoftSatisfactionOf class property describes the relationships between Privilege class of the Regulatory Authority with the Regulatory Requirement class as it gives permission to implement a regulatory requirement but not required to, also the rule has an exception for its compliance in the E-Government system. **Ontology Triple:** *Subject Class:* Policy Document (a), Obligation (b), Privilege (c) (origin: Generic Regulation ontology, OGDL4M ontology (b, c)) *Class Property:* hasOrgRegulationOf (a), hasHardSatisfactionOf (b), hasSoftSatisfactionOf (c) (origin: EGRRC ontology) *Object Class:* E-Gov Service (a), Regulatory Requirement (b, c) (E Service ontology (a), E-Government Literature (b, c))
ONTOLOGY	**E-GIF ontology (Fragkou et al., 2014)**
Ontology Main Focus	The ontology describes the concepts and their interrelationships presented in the ERMIS Greek portal with all the administrative

	public information regarding license provisions.
Class Hierarchy and Class Properties derived from the ontology	**Classes Hierarchy:** • Superclass: Regulatory Source [Subclass: Legal Document] • Superclass: Rule Component [Subclass: Entity] **Class Properties**: • isGoalOf class property describes the relationships between Regulatory Objective class and the Regulatory Source class as most of the E-Government service development goals are coming from various regulatory sources (i.e., legal, policy, agreements provisions) • hasRelationBetween class property describes the relationships between Regulatory Rule (i.e., Fact rule) with E-Government entities as the fact rules describe various relationships between E-Government entities. **Ontology Triple:** *Subject Class:* Regulatory Objective (a), Fact Rule (b) (origin: E-GIF ontology (a), E-Government literature (b)) *Class Property:* isGoalOf (a) hasRelationBetween (b) (origin: EGRRC ontology) *Object Class:* Regulatory Source (a), Entity (b) (origin: EGRRC ontology (a), E-GIF ontology (b))

3.2 Regulatory Requirements in Existing Literature in E-Government

The following table (Table 3) illustrates the ontology elements for EGRRC ontology extracted from existing literature and reports presented in the E-Government and legal domain into two rows. The 'E-GOV DESCRIPTION' gives the literature's reference with the presented concepts in the legal and E-Government regulatory requirements compliance discussed in the literature. And 'EGRRC KNOWLEDGE DERIVATION' provides the derived ontology elements of class hierarchy and class properties to be used in EGRRC ontology.

Table 3: EGRRC Ontology Elements derived from General Published Literature

Literature	Source of Regulations in E-Government system development
Description of the E-Gov Literature in the area of policy and regulations sources	• Alpar & Olbrich (2005); Jansson (2012) discuss the European E-Government policy, enacted by the European Union (EU), that provides the general guidelines of developing interoperable E-Government systems provide service to the citizens and private business organizations to make unified and collaborative public electronic operation under the directory of EU. • Chiriac & Szabo (2014) also discuss the global E-Government

	development Index (EGDI) published every two years by the United Nations (UN) E-Government development database. Mutimukwe et al. (2019) discusses the international privacy standard and practice for the E-Government system development in African countires • Ruhode (2016) discuss ICTs policies of Zimbabwa's government towards developing E-Government System. Zulhud (2012) describes the Malaysian state legal framework in ensuring the security measurement of protected information exchange in E-Government. Kleine (2009) discusses the public state regulations and local government policies introduced in developing the e-procurements system for the Chilean government. • Jaeger (2008) discusses the user-centered accessibility policy of E-Government websites for persons with disabilities from section 508 of the Federal Rehabilitation Act. • Breaux (2010) discusses the US federal E-Government policy on the Health Insurance Portability and Accountability Act (HIPAA) that provides data privacy and security provisions for safeguarding medical information in delivering public service. • Kromidha (2012) discusses that the E-Government projects sometimes take assistance from other than national funds. In that case the agreements with the funding organization are considered as a benchmark in the system development policies. • Kuzma (2010) discusses the World Wide Web Consortium (W3C) that provides E-Government system development guidelines to benchmark the E-Government services and operation into a global standard.
Class Hierarchy and Class Properties Derived from the Literature	**Classes Hierarchy:** • Superclass: Regulatory Source [Subclass: Legal Document, Standard Document, Policy Document, Agreement Document] • Superclass: Stakeholder [Subclass: E-Gov Donor, E-Gov User] **Class Properties**: • hasBestPracticeOf class property describes relationships between Standard Document class with the E-Government Service class as the standard document presents the general guidelines and best practices of the E-Government service development such as HIPPA, W3C. • hasContractualRegulationOf class property describes the relations between the Agreement Document class with the E-Government Service class where the stakeholder such as the donor of the E-Government project has some conditions to finance in the project. • hasAgreementWith class property describes the relationships

	between Agreement Document class with the Stakeholder class as many conditions are made with various stakeholders in order to get their support and finance in the E-Government project development. **<u>Ontology Triple:</u>** *Subject Class:* Standard Document (a), Agreement Document (b, c) (origin: E-Government Literature) *Class Property:* hasBestPracticeOf (a) hasContractualRegulationOf (b), hasAgreementWith (c) (origin: EGRRC ontology) *Object Class:* E-Gov Service (a, b), Stakeholder (c) (origin: E-Gov Literature (a, b), E-Gov Project Management ontology (c))
Literature	**Regulatory Objective in E-Government system development**
Description of the E-Gov Literature in the area of regulatory objectives	• Rehman et al. (2018) discuss the United Nations's sustainable development goals in E-Government system development. Angelis et al. (2010) discuss the regulatory rules for the E-Government system development goal that is expected to achieve in long term future endeavour. • Schmid et al. (2007) says that these long-term general objectives of E-Government system development are often difficult to measure because they represent abstract goals outside of the E-Government system. • Chiriac & Szabo (2014) discusses the E-Government system development policies for free access to government information, government transparency, reducing cost, and strengthening the public administrative capacity. These benefits are expected to be achieved in a relatively short period and they are relatively easy to measure.
Class Hierarchy and Class Properties Derived from the Literature	**<u>Classes Hierarchy</u>:** • Superclass: Regulatory Objective [Subclass: Regulatory Impact, Regulatory Outcome] **<u>Class Properties</u>**: • isGoalOf and hasAgreeementWith class properties describe relationships between Regulatory Impact class with Agreement Document and E-Gov Donor class as this agreement shows the long-term vision of the E-Government system development. **<u>Ontology Triple:</u>** *Subject Class:* Regulatory Impact (a, b) (origin: E-Gov Literature) *Class Property:* isGoalOf (a), hasAgreementWith (b) (origin: EGRRC ontology) *Object Class:* Agreement Document (a), E-Gov Donor (b) (origin: E-Gov literature (a), E-Gov project Monitoring ontology (b))

Literature	Regulatory Rules in E-Government system development
Description of the E-Gov Literature in the area of Regulatory Rules	• Alpar & Olbrich (2005) discusses law regarding automated and manual mode of the actions in performing E-Government operations. Wang et al. (2020) discuss the Even-Condition-Action (ECA) rule in E-Government system development. • Jansson (2012) and Schmidt et al. (2007) discuss the E-Government policies regarding the responsible roles of performing system activities. Schmidt et al. (2007) also discuss the action to be made under specific conditions. • Wiegers and Beatty (2013) discusses regulatory rules that describe the presence of specific structures in the regulatory rules of system operations. For example, the factual information about some important entities in a requirement, action enabling rules that triggers some activities based on conditions, provide restriction and specific mathematical calculation formulas in a system operation.
Class Hierarchy and Class Properties Derived from the Literature	**Classes Hierarchy:** • Superclass: Regulatory Rule [Subclass: Action Rule, Fact Rule, Constraint Rule, Computation Rule] • Superclass: Rule Component [Subclass: Task, Condition, Restriction, Formula, Association] **Class Properties**: • hasAllow class property describes the relationships between the Action Rule/Constraint Rule classes of the Regulatory Rule with the Stakeholder class as it allows various types of stakeholders to interact in the E-Government system. • hasPerform class property describes the relationships between the Action Rule/Constraint Rule classes of the Regulatory Rule with the Task class of Rule Component in performing various tasks in the E-Government systems. • isBasedOn class property describes the relationships between the Regulatory Rule (i.e., Action Rule/Constraint Rule/ Computation Rule/Fact Rule) classes with the Rule Component (i.e., Condition/Restriction/ Formula/ Association) classes in performing various tasks based on condition, restriction, formula, and association exists in the regulation. **Ontology Triple:** *Subject Class:* Action Rule/Constraint Rule (a, b) Regulatory Rule (c) (origin: E-Gov Literature) *Class Property:* hasAllow (a) hasPerform (b), isBasedOn (c) (origin: EGRRC ontology) *Object Class:* Stakeholder (a), Task (b), Rule Component (c) (origin: E-Gov Goal ontology (a) E-Gov Literature (b, c)

Literature	Regulatory Requirements in E-Government system development
Description of the E-Gov Literature in the area of Regulatory Requirements	• Chiriac & Szabo (2014); Bekkers (2009) discuss agreements and policies regarding the implementation constraints of the E-Government information exchange on promoting cooperation between public organizations for delivering one-stop public e-services. • Angelopoulos et al. (2017) discuss the privacy and security requirement of the E-Government systems. Alpar & Olbrich (2005); Goldkuhl (2011) describe the specific requirements of an E-Government system application to fulfill certain purpose and rely on general rules enacted by the public regulations. • Layne & Lee (2001); Prins (2007) argue for protecting the privacy of protected information in E-Government systems and provide security of information exchange over the E-Government public network. • Goldkuhl (2011) describes the policies in the interactions of E-Government service delivery between government agencies as a service provider and citizen as a service receiver.
Class Hierarchy and Class Properties Derived from the Literature	**Classes Hierarchy:** • Superclass: Regulatory Requirement [Subclass: System Requirement Development Requirement] • Superclass: System Requirement [Subclass: Operational Requirement, Quality Requirement] • Superclass: Regulatory Source [Subclass: Policy Document, Agreement Document] **Class Properties**: • hasSystemProperty class property describes the relationships between the E-Government System Requirements with the e-Gov Services class as the regulations may provide some system-oriented expectations in E-Government operation. • hasDevelopmentPropertyOf class property describes the relationships between the Development Requirement class with the E-Gov Service class as it describes various E-Government project constraints in E-Government system development. • hasFunctionalPropertyOf class property describes the relations between Operational Requirements class with the E-Government Services class where the operational requirements describe the functionality of the E-Government system such as firewall and cryptography in system operation. • isOriginatedFrom class property describes the relationships between the Regulatory Requirement class with the Regulatory Source classes as the regulatory requirements are primarily originated from various regulatory sources. For example, Development Requirements are primarily originated from the

	policies and agreements (i.e. internal regulations) • isExternalSourceOf and isInternalSourceOf class properties describe the relationships between External Regulation and Internal Regulation classes of Regulatory Source with the Regulatory Requirement class. The external regulations (i.e., legal, and standard documents) are not directly enacted for the implementation of a particular E-Gov project development whereas the internal regulations (i.e., various types of policies ad agreements documents) provide various types of requirements for a particular E-Government system development. **Ontology Triple:** *Subject Class:* System Requirement (a), Development Requirement (b), Operational Requirement (c), Regulatory Requirement (d), External Source (e), Internal Source (f) (origin: E-Gov Literature (E-Gov literature (a, b, c, d), EGRRC ontology (e, f)) *Class Property:* hasSystemProperty (a), hasDevelopmentPropertyOf (b), hasFunctionalPropertyOf (c), isOriginatedFrom (d), isExternalSourceOf (e), isInernalSourceOf (f) (origin: EGRRC ontology) *Object Class:* E-Gov Service (a, b, c), Regulatory Source (d), Regulatory Requirement (e, f) (origin: E-Service ontology (a, b, c), EGRRC ontology (d), E-Government Literature (e, f))
Literature	**Prioritization of Regulatory Requirements in E-Gov system development**
Description of the E-Gov Literature in the area of Prioritization of Regulatory Requirements	• Alpar & Olbrich (2005); Breaux & Anton (2008) propose methods that discuss the use of conjunction operators in E-Government regulations to describe the compound rules which connect functions and events in the E-Government system operations. Breaux & Anton (2008) also proposes a method to extract the E-Government access rights and obligation from United States enacted legislation (e.g., HIPAA). • Olbrich & Simon (2008) models the rights and obligations of Swiss E-Government regulatory rules. Also, it discusses the dependencies among the rules in the regulation. • Massey et al. (2009) discuss the priority level of legal requirements in terms of legal implications and priority score. The legal implication is defined by the cost of non-compliance with the legal requirements whereas the priority score is defined by the number of subsections and exceptions used in the regulatory rules.
Class Hierarchy and Class	**Classes Hierarchy:** • Superclass: Compliance Priority [Subclass: High Priority, Low Priority] • Superclass: Rule Complexity [Subclass: Simple Rule,

Properties derived from the Literature	Compound Rule] • Superclass: Compliance Probability [Subclass: Total Compliance, Partial Compliance] • Superclass: Regulatory Authority [Subclass: Obligation, Privilege] **Class Properties**: • hasPriorotyOf class property describes relationships between Compliance Priority and Regulatory Requirements class as it defines the priority of the regulatory requirements coming from various sources. • hasProbabilityOf class property describes the relationships between Compliance Priority class with the Compliance Probability class. This relationship describes the necessity of regulatory compliance as all the regulatory requirements do not need to be compliant in the E-Government system development. • hasSeverityOf class property describes the relationships between Compliance Priority class with the Compliance Impact class. This relationship explains the consequence of non-compliance with the regulatory requirements in the E-Government system development. • hasComplianceOf class property describes the relationships between the Compliance Impact (i.e., Significant, Negligible) with the Regulatory Authority (i.e., Obligation, Privilege) class. • hasSatisfy class property describes the relationships between Regulatory Authority class with the Regulatory Requirement class as the obligation and privilege of the regulations describes the required satisfaction level of the regulatory requirements in the E-Government system development. • hasHardSatisfactionOf class property describes the relations between the Obligation class of Regulatory Authority with the Regulatory Requirement class as it requires completely 100 percent compliance of the regulatory requirement in the E-Government system development. • hasSoftSatisfactionOf class property describes the relations between the Privilege class of Regulatory Authority with the Regulatory Requirement class as it gives permission to implement a regulatory requirement but not required to, also the rule has an exception for its compliance in the E-Government system development. **Ontology Triple:** *Subject Class:* Compliance Priority (a, b, c), Compliance Impact (d), Regulatory Authority (e), Obligation (f), Privilege (g) (origin: E-Gov Literature (a, b, c, f, g), EGRRC ontology (d, e)) *Class Property:* hasPriorityOf (a), hasProbabilityOf (b), hasSeverityOf (c), hasComplianceOf (d), hasSatisfy (e),

	hasHardSatisfactionOf (f), hasSoftSatisfactionOf (g) (origin: EGRRC ontology) *Object Class:* Regulatory Requirements (a, e, f, g), Compliance Probability (b), Compliance Impact (c), Regulatory Authority (d) (origin: E-Gov literature (a, e, f, g), EGRRC ontology (b, c, d))
Literature	**Evolution of Regulatory Requirements in E-Government system development**
Description of the E-Gov Literature in the area of Evolution of Regulatory Requirements	• Sulistiyani & Susanto (2018) discuss the change management of E-Government system development due to policy and regulation amendments. Gómez-Pérez et al. (2006); Angelis et al. (2010) discuss the changes in E-Government policies and objectives from the efficiency of a government operation to the effectiveness of E-Government system to the civil society. • Alpar & Olbrich (2005); Prins (2007) discuss the amendment of regulations for digital signature in electronic operation. Alpar & Olbrich (2005) also discuss the modifications of laws are relatively easy to achieve in internal regulations that affect short term changes in the internal workflow in the electronic system. This type of modification is mostly done by the organization by themselves. On the other hand, there are some public laws that contain rules for the institution in general terms which should be approved by the legislature in a long run procedure with political and social influence. • Khadraoui et al. (2008) discusses the importance of establishing links between legal sources to the E-Government services as the regulations are evolving fast for the dynamic nature of regulations due to amendment, abrogation, and introducing new laws in the E-Government service development.
Class Hierarchy and Class Properties derived from the Literature	**Classes Hierarchy:** • Superclass: Rule Status [Subclass: Static Rule, Dynamic Rule] **Class Properties**: • isOriginatedFrom class property describes relations between regulatory Rule Status with the Regulatory Source class as the status of the regulatory rules (i.e., static rules or dynamic rules) are defined by various types of regulations (i.e., policies, agreements, legal provisions, standards). • hasResult class property describes the relationships between Internal Regulation and External Regulation class with the Dynamic Rule and Static Rule class as the E-Government system is often reconfigured for the adaption of any changes made in the policies and agreement documents (i.e., internal regulation) whereas the external regulation such as legal and standard are not very often subject to changes.

	Ontology Triple: *Subject Class:* Rule Status (a), Internal Regulation (b), External Regulation (c) (origin: EGRRC ontology) *Class Property:* isOriginatedFrom (a), hasResult (b, c) (origin: EGRRC ontology) *Object Class:* Regulatory Sources (a), Dynamic Rule (b) Static Rule (c) (origin: EGRRC ontology (a), E-Gov Literature (b, c))

Furthermore, Table 4 presents the summary of the triple descriptions in reutilizing, extending, and combining the existing vocabularies from the available ontologies to enhance their reusability and extension through the EGRRC ontology. This is particularly useful in adapting to the concept of Linked Data paradigm while avoiding duplication of information (Bizer, 2009). In that context, EGRRC ontology defines a few subjects and objects classes where needed but mainly deals with defining new relationships (75 in total) through the use of 45 introduced predicates, acting as a link between the various concepts.

Table 4: Summary of the EGRRC Triple description

Triple Descriptions	**Total Number**
Number of ontologies and general published literature used in the EGRRC ontology to import/extract concepts (ontology – 24, Literature – 27)	51
Number of subject classes from imported ontologies and literature	33
Number of subject classes newly defined in EGRRC ontology	9
Number of object classes from imported ontologies and literature	29
Number of object classes newly defined in EGRRC ontology	10
Number of predicates (i.e., class properties) from imported ontologies	4
Number of predicates introduced in EGRRC ontology to define relationships	45
Number of relations made in the EGRRC (i.e., between subject-object class)	75

3.3 EGRRC Ontology Description

From the existing ontologies and general published literature in the E-Government domain presented in Table 2 & 3, various concepts of regulatory requirements compliance are extracted. The regulatory requirements for e-services are originated from various regulatory sources that describe various policies and regulatory documents enacted by the local, regional, national, and international authorities. The

objectives of policy and regulations describe various goals of the regulatory requirements. The policy and regulation affect various types of E-Government services which provide electronic services to various groups of the service recipient. There are various types of regulatory requirements originated from policy and regulations, some of them describe the systems properties and others describe the development process of e-service. The structures of rules are also discussed in formulating regulatory requirements based on various rules components in the policy and regulation. The regulations are also discussed in various types of complexities in the rules and consequences of any non-compliance in order to understand the impact of non-compliance and prioritize the regulatory requirements accordingly. Finally, the maturity of the regulatory requirements is also discussed in the context of evolving policy and regulation from various authorities. The next section will describe the EGRRC ontology based on the derived concepts from the existing ontologies and general published literature in E-Government.

Based on the ontology elements presented in existing ontologies and general published works in the E-Government domain (Tables 2&3), the EGRRC ontology is proposed to describe various interconnected concepts of regulatory requirements compliance in E-Government system development using protégé. The extracted data were analyzed in the following criteria which answers several queries regarding E-Government regulatory requirements compliance.

Q1: What are the sources of regulatory requirements in the E-Government system development?
Q2: What are the regulatory documents that present internal and external sources of regulatory requirements?
Q3: What regulatory documents present agreement with various stakeholder and what is the agreement length validity?
Q4: What are the objectives of regulatory requirements in the E-Government system development?
Q5: What are the long-term abstract and short-term immediate goals in the E-Government system development requirements?
Q6: What types of E-Government services are affected by the regulatory requirement?
Q7: What are the types of regulatory requirement in the regulation need to be compliant in the E-Government system development?
Q8: How regulatory rules are formulated in the E-Government requirements?
Q9: What are the constraint or prohibitions that made upon various E-Government system development tasks and stakeholders?
Q10: How to prioritize the E-Government regulatory requirements?
Q11: What regulatory rules remain stable in the E-Government system operation what rules are subject to change in further modification?
Q12: What regulatory documents presents static and dynamic rules?

3.3.1 Sources of E-Government Regulatory Requirements

The origin of E-Government regulation answers the query of finding the regulatory requirements in E-Government system development from multiple sources. It distinguishes and discusses various sources of E-Government regulatory requirements which can be classified into two main categories of Internal regulations and External regulations (Figure 10).

Internal regulations: The regulations those are coming from the sources where the E-Government system is being developed are the internal or intra-organizational regulation. Here the E-Government organizations are directly involved in the creation and amendment process of their own regulations. It provides the regulatory requirements of E-Government system development from various organizational policies and contract agreements. For example:

```
Policy Name: System development policy,
             System promotional policy,
             User policy,
             Admin policy.
```

Every organization may have its own policies regarding the digitization of their operations. Here, the system development policy defines the operational goal and system development constraint in the E-Government service development. The system promotional policy defines how the E-Government services are promoted to the citizens and business organizations in their interactions with the government agencies. User Policy provides the regulations about how a user can use the E-Government system. Admin Policy provides the regulation about how the resources are to be used in the E-Government system development. These policies are enacted by the individual public organization in the regional or state level where the E-Government system is being developed. The internal regulation also covers several service level agreements with government agencies and various stakeholders involved in developing the E-Government system projects.

```
Agreement Name: User agreement,
                Donor agreement,
                Vendor agreement,
                Collaboration agreement.

Agreement Length: six months, one year.
```

The agreement defines a contract between the organization who initiate the E-Government project development with the users who demand the E-Government service such as citizens and business organizations, donors who aid in the development of the projects such as European Union (EU), charitable non-profit private organization (NGO) who partially or fully funds the E-Government system

development projects, ICT vendors who provide technical resources and services to the E-Government system development, collaborative organizations are the other public organizations who support in the E-Government system development, for example, in providing one-stop E-Government services where multiple public organizations work and interface with one another. Furthermore, the agreement length defines the validity period of the conditions presented in the agreement documents which may renegotiate after six months or one year timespan depending on the validity length of the agreements.

External regulations: the regulations those are coming from the external sources of the organization where the E-Government system is being developed and not directly involved in the creation and amendment process of the regulation are the external or extra-organizational regulations. It provides the regulatory requirements of the E-Government system development from various E-Government system development standards and authoritative legal instructions in the national or wider level which are outside of the E-Government organizational parameter.

```
Standard Name: Web2.0 technology in interface design,
               Web services technical standard.
```

Here, the web 2.0 technology is an international standard for web interface design of a public web portal that may consider in the E-Government system development as a general guideline to be compliant with the international standard of E-Government system development such as maintaining usability issues for disabled people in designing a public website. Similarly, web services technical standards may also consider in the E-Government system development in information exchange for maintaining interoperability of various systems to communicate with each other in providing one-stop E-Government services to the citizens and business organizations. The external regulation also covers the authoritative legal instructions enacted by the local or state government.

```
Legal Document Name: National ICT regulations,
                     General Data Protection Regulation,
                     Health Insurance Portability and
                     Accountability Act (HIPPA),
                     Sarbanes–Oxley Act (SOX),
                     Gramm-Leach-Bliley Act (GLB).
```

There are some judicial rules from the government which should be compliant in the E-Government system development. For example, The National ICT regulation presents the nationwide E-Government system development principles enacted by the government such as the HIPPA (Health Insurance Portability and Accountability Act of 1996) legislated in the USA in e-Health system development to be compliant with data privacy and security provisions for safeguarding medical information. The new

General Data Protection Regulation (GDPR) enacted by the Council of European Union presents the data privacy law in protecting the rights of using an individual's personal data across the European member states countries. Sarbanes Oxley Act of 2002 also known as Public Company Accounting Reform and Investor Protection Act is a United States federal law that sets the rules for any public organizations to protect shareholder's interests from any sort of accounting errors in the business operations and fraudulent practices in enterprises and also to improve the accuracy of corporate information disclosures. The Gramm Leach Bliley Act (GLBA) which is also known as the Financial Services Modernization Act enacted in the year of 1999 by the United States Congress for federal home loan banking system operations to provide a framework for the banking organizations, securities companies, and any other financial services providers.

Moreover, identifying the sources of regulation helps the E-Government system analyst in re-negotiating the terms and conditions by understanding the origin of regulations in the E-Government system development. For example, the intra-organizational regulation may re-negotiate if necessary upon the completion of agreement period or consensus among the stakeholders involved in the project whereas the extra-organizational regulations are very hard to re-negotiate in the E-Government system development.

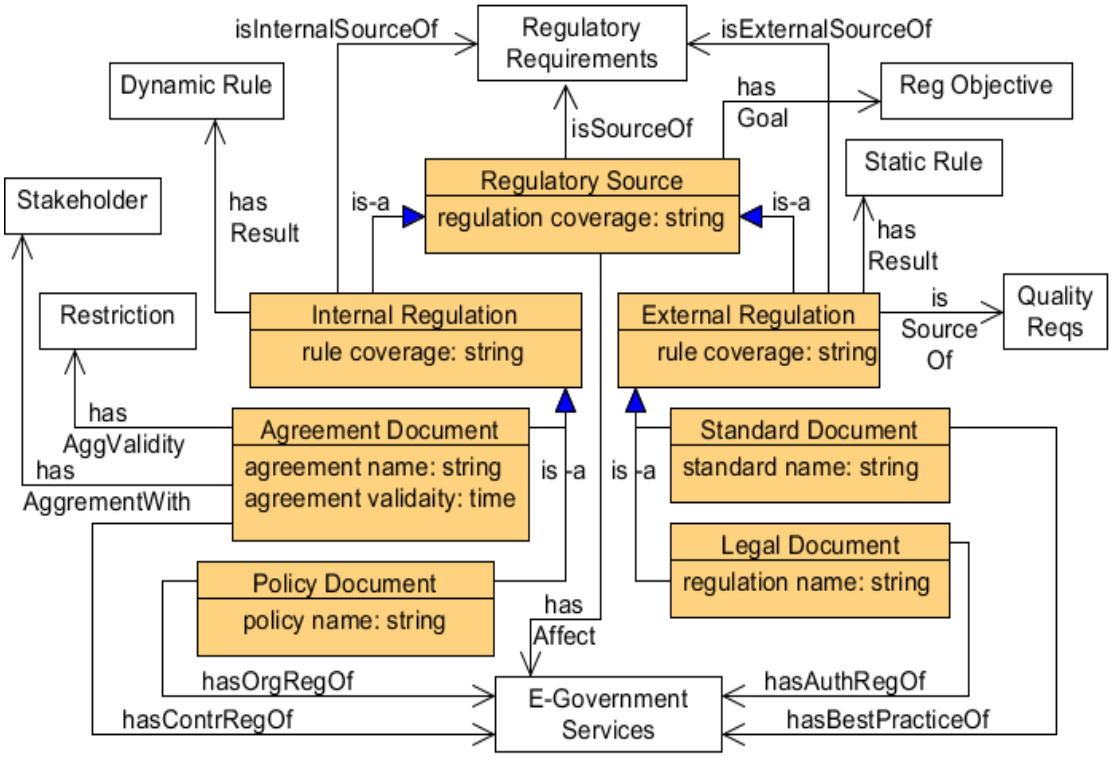


Figure 10: Source of E-Government Regulatory Requirements

The regulations from both internal and external sources affects the E-Government services as the regulations from various sources can impose the goals and objectives of the implementing E-Government systems. Furthermore, the regulations also

impose necessary requirements of the E-Government system development where the external source of regulations are particularly imposing the non-functional requirements or quality attributes and constraints of the E-Government system development.

Furthermore, the regulatory document contains several sections of regulations where it is not always necessary to comply with all the sections in an E-Government system development. Therefore, after identifying various related regulatory documents, the E-Government system analyst may need to look for the related sections of regulations in the regulatory document.

```
Regulation Coverage: Individual regulatory document,
                     Section of an act in the document.
```

Here, the coverage of regulations can be the whole regulatory document such as the organization's system development policy to develop an E-Government system, or a section of a regulatory act such as the rules regarding privacy and security issues of E-Government information transaction enacted by National ICT policy. It is very often noticed that the entire set of rules from a regulatory document might not necessarily to be implement in the system development where just a part of the regulation document may be applicable in the system development.

3.3.2 Objective of E-Government Regulatory Requirements

The regulatory requirements from different sources of regulatory documents have various regulatory goals or objectives in the E-Government system development projects. The objectives of the regulatory requirements in the E-Government system can be classified into two primary categories according to its goal that needs to be fulfilled in the E-Government system development projects (Figure 11).

Regulatory Impact: The regulatory requirements that generally present the vision statement of the E-Government system development objective is the Impact or Effectiveness of the E-Government projects. It defines the overall abstract goals of the regulatory requirements those have to be realized within the E-Government system development in the long run operation (i.e., the effectiveness of the E-Government system operations).

```
Regulatory Impact: Transparent government,
                   Quality of citizen's lives,
                   Improve business operation.
```

Here, the transparent government refers to achieve citizen's trusts on government by providing information and make government operations visible to the citizen and business organization, quality of citizen's and business life defines the goal of increasing the satisfaction level of the citizens and business organizations who receive

services from the public organization as the ultimate purpose of E-Government system development is to improve the lives of citizens, and the operations of business organization with the government.

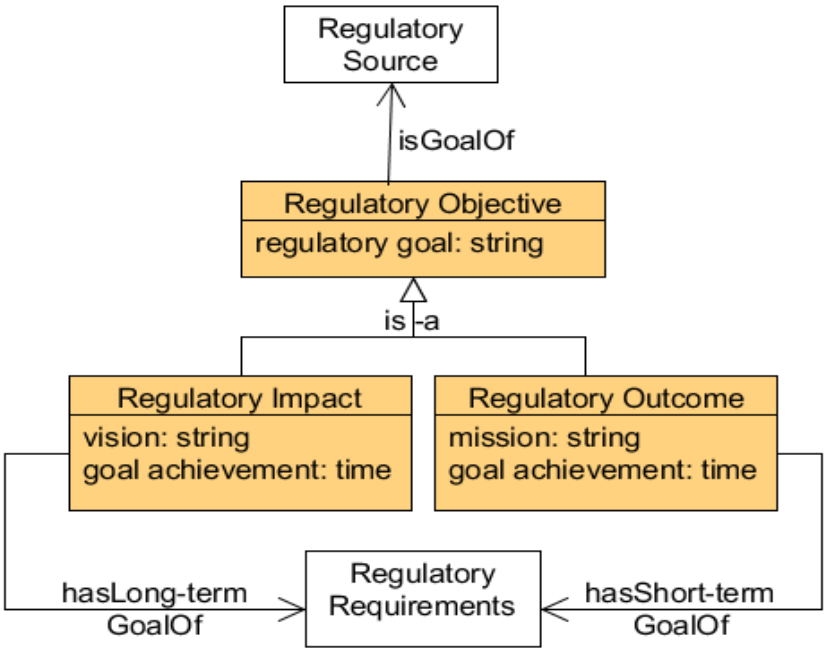


Figure 11: Objective of E-Government Regulatory Requirements

Regulatory Outcome: The regulatory requirements that present the mission statement of the E-Government system development objective is the Outcome or Efficiency of the E-Government projects. It defines the immediate goals of regulatory requirements that need to be satisfied in the E-Government system development.

```
Outcome: Efficiency of government operation,
         Reduce workload and operational cost,
         Provide information access,
         Reduce waiting time.
```

Here, the efficiency of government operation defines the goal of E-Government system development in increasing the productivity of government operations by introducing the electronic means of doing their work. Reduce workload and operational cost refers to the E-Government system development objective as minimizing the working pressure and operational expenses by introducing the electronic system, for example, the government tax office wants to reduce the staff cost 25 percent by introducing online income tax return system through their website. Information access refers to the objective of E-Government system development as providing government information to its citizen and business organization, for example, the government tax office provides necessary information regarding income tax to the citizen and business organization through their website. Reduce waiting

time refers to the objective of E-Government system development as quick service delivery to the service recipient without having been waiting them for a long time in the service desk queue.

3.3.3 Regulated E-Government Services

The e-services are delivered to various user groups in fulfilling their specific goals while using the E-Government system. The E-Government services are generally fulfilling the short-term immediate goals of the E-Government system that originated from various regulations. The E-Government system delivers primarily three types of e-services to different E-Government user groups in responding to their service request (Figure 12). For example, the services providing from the government organizations to the citizens are as follows.

```
Government-to-citizen (G2C): E-Driving License,
                             E-Passport,
                             E-Railway Ticket.
```

Here, the Government-to-Citizen (G2C) e-services provide the E-Government services to the citizens. For example, the e-Driving License system provides online services to the citizens to make application and submit all necessary documents for issuing driving license for the citizens. The citizens of a country can also apply for their national passport through online by the e-Passport system. The e-Railway Ticket system serves the citizens to purchase tickets for their railway journeys through online. Here, the goal of the G2C services is to reduce the citizen's waiting time to get quick public services.

The Government-to-Business (G2B) provides electronic E-Government services to the business organization in performing their business operation collaborating with the government agencies. Some examples of the government services to the business organizations are as follows.

```
Government-to-Business(G2B): E-Trade License application,
                             E-Tender application,
                             E-Tax Return submission.
```

In the G2B E-Government services, the e-Trade License system provides E-Government service to the business organizations to apply for trade license through online. The e-Tender system provides electronic services to the business organizations to make online bidding for government projects. The e-Tax Return system provides electronic services to the business organizations to submit their TAX/VAT related information and files to the income tax office through online. Here, the primary goal of G2B services is to provide access to information in doing business operations and reduce waiting time to get public services by the business organization.

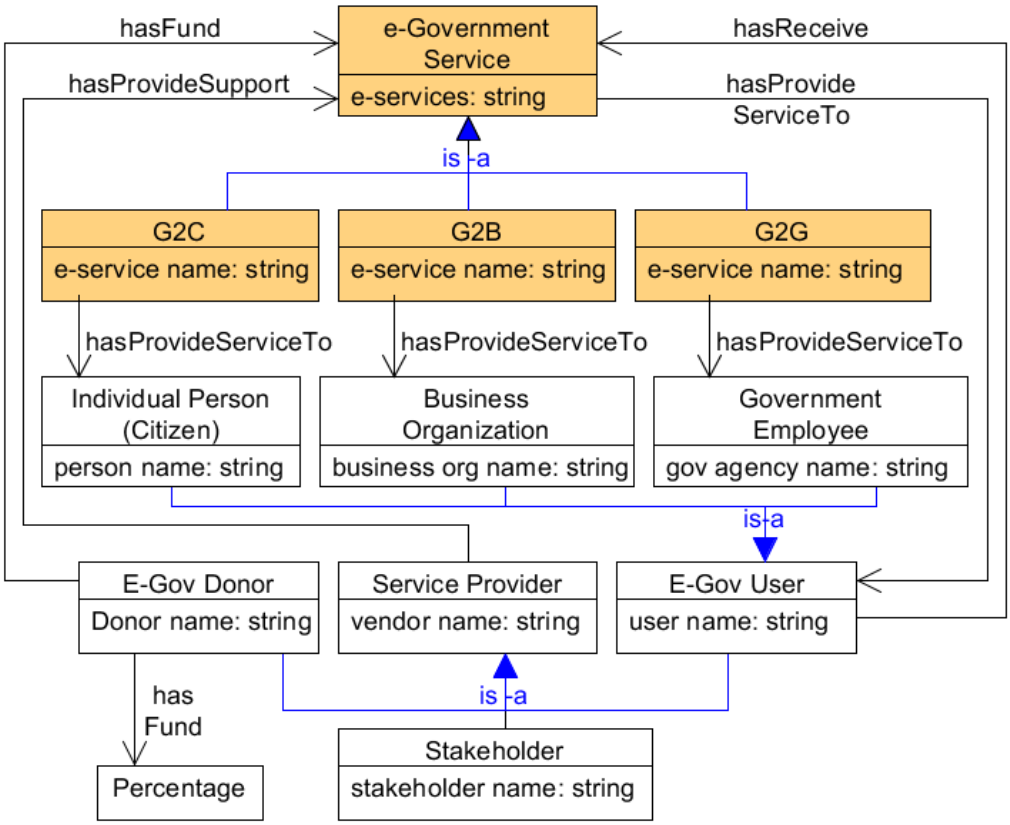


Figure 12: Regulated E-Government Services

Finally, the Government-to-Government (G2G) E-Government service provides electronic services to the employees of a government agency. Some examples of the government services to the employees of the public organizations are as follows.

```
Government-to-Business (G2G: E-Payroll System,
                            E-Profiling System,
                       Online unemployment insurance.
```

Here, the e-Payroll system provides electronic services to the government agencies to manage their employee's salaries and other employee benefits. The e-Procurement system provides electronic services to the government agencies to manage the procurement process of products and services from third party business organizations. Furthermore, a government agency may also provide electronic services to other government agencies. For example, the e-Profiling system provides electronic services to the law enforcement agencies in accessing data from the population register agency through online services while profiling a criminal or victim. The online unemployment insurance system provides electronic services to the office of labor and unemployment agency to access health information from the public health care agencies. Here, the G2G e-services are reducing the workload of the government employees, reduce the operational costs, improve the efficiency of government operations, and ensure reliable service delivery process to the service recipient.

Furthermore, the E-Government Stakeholder can be the Donor or Sponsor who provide financial support in the E-Government system development projects. It also describes who funds about what percentages in the E-Government service development project if there are multiple Donors. Another E-Government stakeholder is the Service provider who provides support and service in the E-Government system development where the IT Vendor provides all the technical supports, and the Government Agencies provide collaborative support to the system development.

3.3.4 E-Government Regulatory Requirements

The regulatory requirements describe various properties of the E-Government services and the system development from the regulatory rules originated from various regulatory documents. There are several types of regulatory requirements that need to be compliant in the E-Government system development (Figure 13). Identifying these categories of regulatory requirements is often helpful for the E-Government system analyst in understanding the nature of the requirements in order to ensure their compliance in the E-Government system development.

E-Government system requirements: the regulations that describe the properties of the E-Government system into its functional, quality, and interfacing requirements are the system requirements. It describes product details of the E-Government system development in technology specified conditions and in general operational conditions. The technology specified requirement refers to any precise technology is required in providing the E-Government services such as the use of mobile phone messaging to give public information access to citizen and business. This information can be particularly useful in the choice of selecting alternative technologies in the E-Government system development. Product requirements can be further classified into Functional requirements and Non-functional requirements.

Functional requirement: It specifies the operational behavior of the E-Government system that exhibit under a specific condition in the E-Government system operation, the function that a system shall perform. The functional requirements define the system operation performed by the E-Government users by manual operation or the system by itself in automated actions on the e-service processing and delivery.

```
Functional role: user, system.

Functionality: operational tasks.
```

For example, the system shall verify the national identity number (NID) of a taxpayer individual or business organization to provide access to online submission of his/her online tax return form. And, the taxpayer shall have to apply for tax identity number (TIN) before submitting the tax file in online, etc.

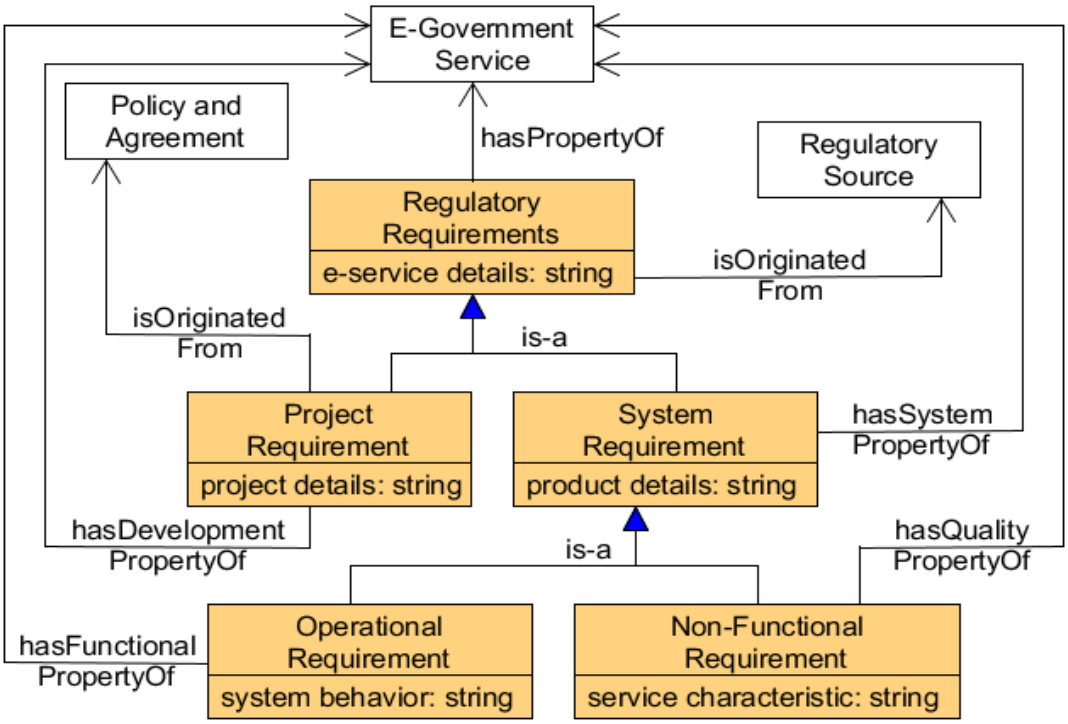


Figure 13: E-Government Regulatory Requirements

Non-Functional requirements: the regulations also refer to the quality of the E-Government system known as non-functional requirements which describe how the system will perform its functional requirements or operations. For example, availability, performance, security, usability, etc.

```
System characteristic: system availability,
                       system performance,
                       system security,
                       system usability.
```

Here, the availability requirements define to the percentage of uptime of an E-Government system in a given duration, for example, the E-Government system shall be available at least 95 percent time in between 10:00 AM to 5:00 PM local during weekdays. The performance requirements define how well the E-Government system shall perform some specific operations, for example, an E-Government electronic form shall be downloaded in less than 10 seconds, or the authorization process of an E-Government transaction shall not take more than 10 seconds. The security requirements define the prohibition of unauthorized access to the E-Government system, for example, only the admin privilege users of the e-Tax system can modify the tax calculation formula in generating individual's tax return documents. The usability requirements define that a user shall be able to submit tax return form in an average of 8 to 10 minutes.

E-Government project requirements: the regulations primarily originated from the internal regulations such as policy and agreement documents also refer to the

requirements of the E-Government project development. Project requirements define the constraints that need to be followed by the project management team during the project development.

```
Project details: Project collaboration,
                 Training for user and development staff,
                 Project deliverable,
                 System maintenance.
```

Here, project collaboration refers to the regulations regarding collaboration between several public and private organization in resource sharing and provide one-stop E-Government service. The training requirement refers to exercising the recommended training including training materials in the project development team and user groups. The project deliverable refers to the regulations regarding the scope and deadlines of implementing the E-Government system. The system maintenance requirement refers to the review and modification of the E-Government system over time such as new security measurement implementation to ensure the appropriate protection of protected electronic information.

3.3.5 E-Government Regulatory Rules

A taxonomy of regulatory rules is particularly helpful for the system analyst to identify the rules and conditions regarding the requirements of E-Government system development that the system developer might not have thought of otherwise. Moreover, classifying the regulatory rules also provides the system analyst an indication of applying the regulatory requirements in the E-Government system development. The regulatory rules can be decomposed further into the categories of Facts rules, Action rules, Constraint rules, and Computation rules in order to fulfill the purpose of the outcome of E-Government regulations (Figure 14). Furthermore, the taxonomy of regulatory rules will also be helpful to extract the regulatory requirements in E-Government system development.

Fact Rule: It describes the relationships between important entities in the E-Government system in formulating the meaningful data model of the system development. The data model would be useful for the E-Government system development to understand the various entities.

```
Entity: System user, System component.
Association: ID number, Service requirest number.
```

Several entities in the E-Government systems are connected with one other using association relationships. For example, every income taxpayer has a unique tax identification number (TIN) in online tax return system, here the entity taxpayer has a relationship with the online tax return system by a unique identification number. Every request submitted by the user has a service request number, here the

identification number of each service request made by the users would help to track the service request uniquely in providing e-services.

Action Rule: It defines the regulatory rules that trigger some activities to be performed by the user role in manual operation or the system by itself in automated operation while a specific condition is true. The rule might lead to specifying an E-Government application functionality exhibits by the E-Government system while detects the triggering event.

```
Role: System user, System component.
Task: Submit, Notify.
Condition: If, While.
```

For example, if the taxpayer has not submitted tax return within the deadline, the system shall notify the taxpayer through an e-mail. In this example, the notification is automated, but the taxpayer also can be notified by the tax collector sending the taxpayer a letter is an alternative manual way of notification while the condition is true (i.e. deadline is expired).

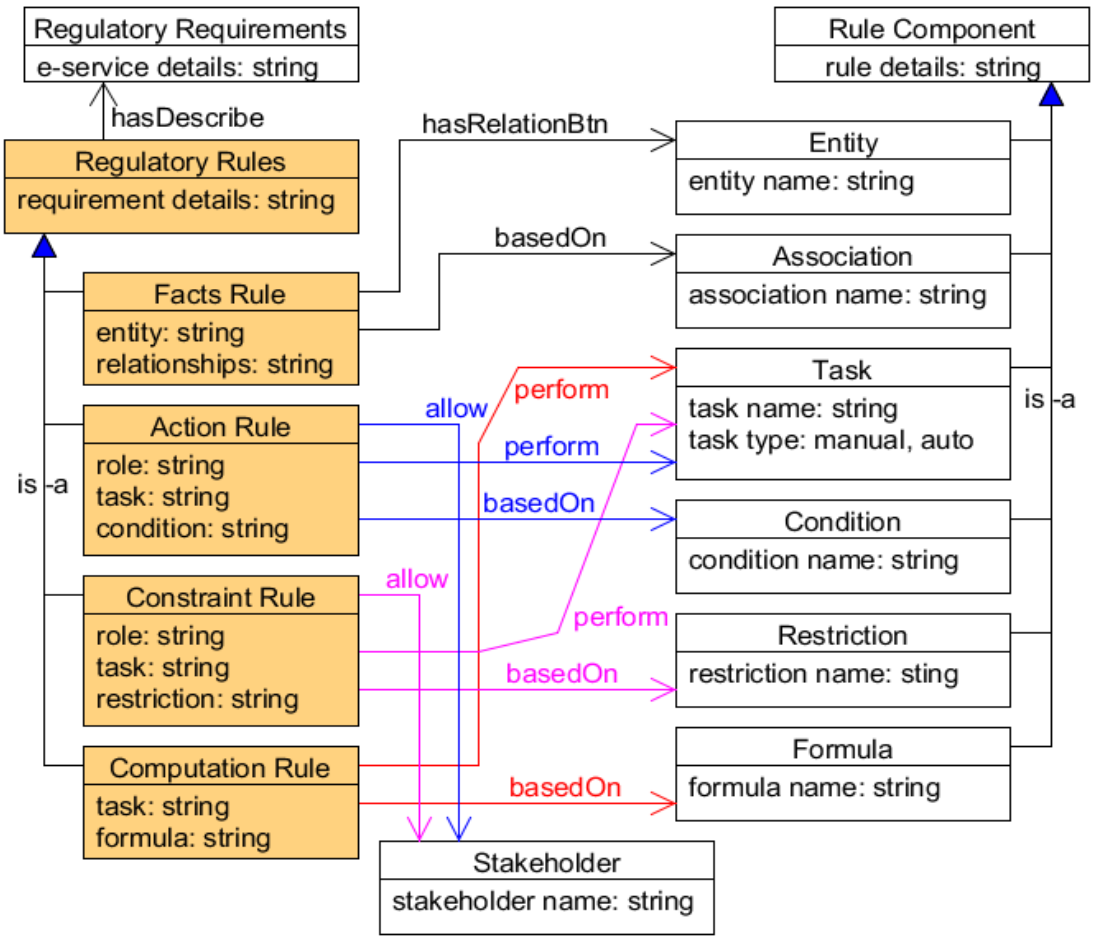


Figure 14: E-Government Regulatory Rules

Constraint Rule: It defines the restriction of an action that the system or the system users are allowed or prohibited to perform. The E-Government regulation describes the constraint rules as certain actions must/must not or may/may not performed by only certain roles specified in the regulation while a condition becomes true.

```
Role: System user, System component.
Task: Login, Submit, Report.
Restriction: Time, Accessibility privilege.
```

For example, the income tax return must be postmarked by midnight on the first office day after November 30th unless an extension has been granted by the tax officer, who has administrative privilege on allowing extension in the system. Here, the task is extending tax return date, role is the tax officer, and the restriction is only the tax officer access privilege can make the extension.

Computation Rule: It defines the regulatory rules regarding the arithmetic computational formula or algorithms that guide the systematic calculation and transform the existing set of data input into new data output in the E-Government system operations.

```
Task: Login, Registration, Submit.
Formula: Mathematical formula, Algorithm;
```

For example, an income taxpayer will submit his/her tax return through online application which is the sum of 15 percentages of his basic salary less the 15 percent of his investment up to 30 percent of his income. Here, the E-Government income tax system shall automatically calculate the total payable amount of income tax of the specific taxpayer.

3.3.6 Priority of Regulatory Requirements

Often the regulatory requirements collected from various sources are inconsistent with one another as well as may contradict along with the system requirements specification in E-Government system development. While there is a contradiction among objectives of regulatory requirements or with the system specifications, the prioritization of the regulatory compliance plays a significant role in measuring the impact of non-compliance in avoiding unpleasant events that will take place for non-compliance with the regulatory requirements (Figure 15).

```
Compliance priority: High priority,
                     Low priority.
```

Here, a higher degree of compliance priority refers to the mandatory compliance that the E-Government system must ensure the rules presented in the regulations at any cost, the lower degree of compliance priority refers to the optional compliance that the regulatory rules can be avoided in the E-Government system which will not cause any

harm in the system development. The compliance priority or regulatory requirements depends on the probability of non-compliance and the impact of non-compliance.

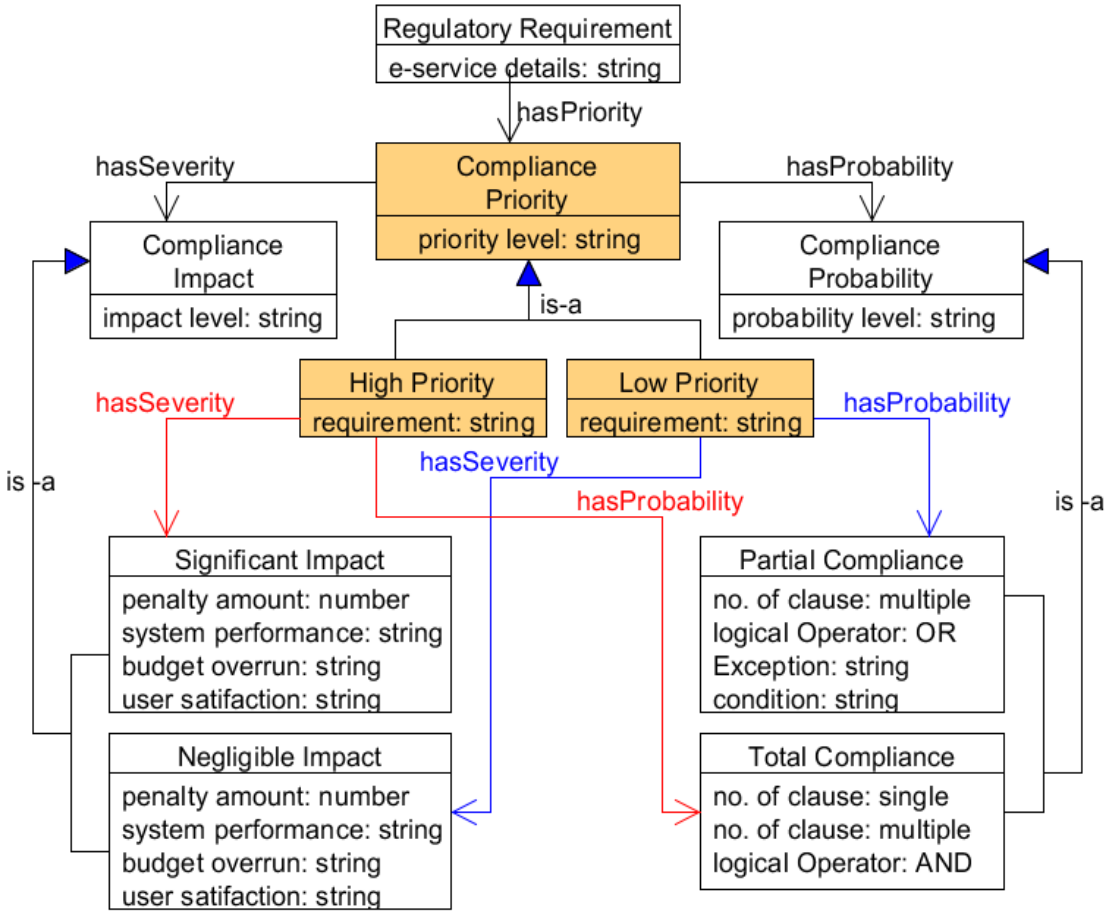


Figure 15: Priority of E-Government Regulatory Requirements

Probability of non-compliance: The probability defines the type of regulatory compliance that refers to how likely the regulatory rules are necessary to be compliant in the E-Government system development and its operations.

```
Compliance probability: Total compliance,
                        Partial compliance.
```

The probability of compliance is defined as total compliance where the regulatory rules that have only a single clause in it which need to be compliant in the E-Government system development (e.g. rule 1, clause 1). Furthermore, the total compliance also refers to the regulatory rules that combine a set of clauses into it (e.g., compound rule) and all of these principles in the compound rule are required to be compliant in the E-Government system (e.g. rule 1, clause 1 AND clause 2). The probability of partial compliance is defined as where there is the compound regulatory rule that combines a set of clauses into it and all of these principles are NOT required to be compliant in the E-Government system development (e.g., rule 1, clause 1 OR clause 2; rule 2, clause 1 EXCEPT clause 2). The compound rules define the available

alternative options of clauses in the rule, exception clauses in the rule operation, and conditions to be applied in the operations of the regulatory rules.

Impact of non-compliance: The impact defines the consequence of non-compliance with the regulatory rules in the E-Government system development.

```
Compliance impact: Severe impact of non-compliance,
                   Negligible impact of non-compliance.
```

The severe impact defines the obligations of the required action or system behavior in the E-Government system and failure to comply with these rules will impose an enormous amount of financial penalty, budget overrun, degradation of technical performance and user dissatisfaction, etc. On the other hand, the negligible impact defines the privileges regarding the action or system behavior that is allowed in the E-Government system, but not required and failure to comply with this rule will not impose any penalty or degrading the system performance.

3.3.7 Maturity of Regulatory Requirements

As time passes, some of the regulations regarding E-Government systems may enforce the adjustment for requirements changes in developing or already developed systems. Hence, the regulations can also be classified into Static and Dynamic regulation based on the probable nature of regulation changes/amendments (Figure 16). This classification can help the E-Government system developer to be aware of possible regulation amendments during the time of E-Government project development and afterward.

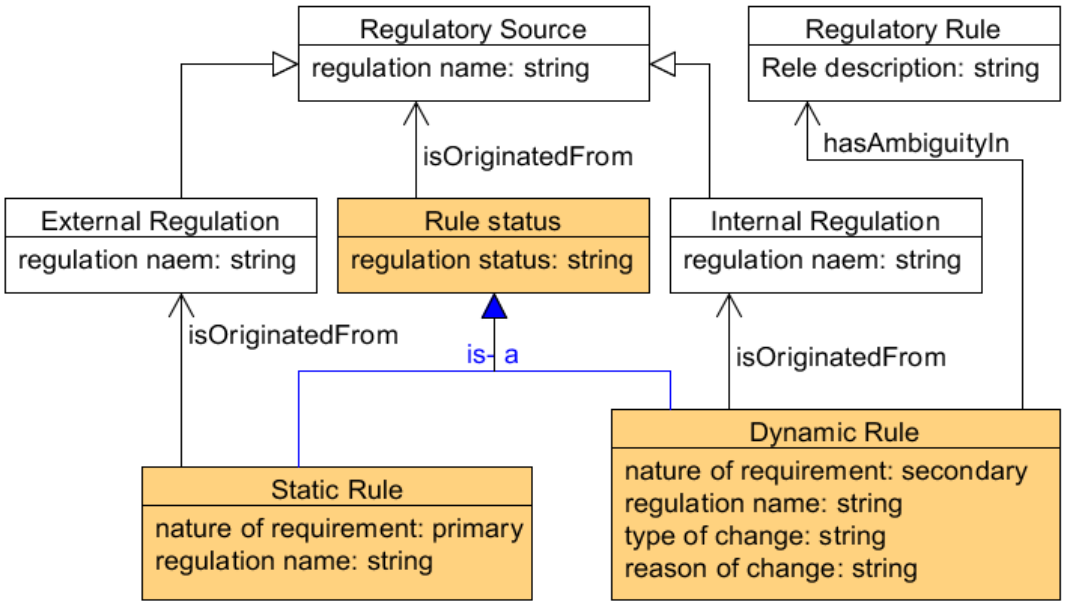


Figure 16: Maturity of E-Government Regulatory Requirements

Static Regulation: The regulatory requirements originated from the static regulations are not often subject to change in the E-Government system development. These requirements are mainly the primary properties of the E-Government systems and mainly originated from the external source of regulations in an E-Government regulation domain.

```
Nature of requirement: Primary system functionalities,
                       Core system functionalities.
```

These are the essential core system's functionalities which lead to the primary objectives in the E-Government system development. Incapable of complying with these requirements will result in a failure to the E-Government project development.

Dynamic Regulation: The regulatory requirements originated from the dynamic regulations are often more subject to changes in the E-Government system development. These requirements are originated from mainly the dynamic rules and regulations from the internal source of regulation in an E-Government domain.

```
Nature of requirement: Secondary, Evolving.
Type of change: Addition of new rules,
                Modification/Abrogation of existing rules.
Reason of change: Technology change, Organizational
                  influence, Political influence.
```

In agile software project development, the primary regulatory requirements are defined at the earlier iterations of project development which represents the main objective of the E-Government system development. On the other hand, the requirements that are mainly secondary to the E-Government system may not very well defined at the earlier time of project development which evolve during the project development time for its incompleteness and inconsistency in policy and regulation. These requirements are specified, enhanced, corrected, and completed depending on technological enhancement, organizational culture, user behavior, and political influence over the course of time.

3.4 Class Hierarchy of EGRRC Ontology

Classes are the main building blocks of an OWL ontology which are sets of individuals. Class hierarchy describes the collection of classes where the specific subclasses are described under the general purpose of super classes. In OWL, the class Thing is the parent of all classes in the ontology. Therefore, all the classes in the ontology are the subclasses of the Thing class. Although, there are no specific naming rules for classes in the ontology, however, it is recommended that the class names should start with a capital letter without containing any spaces in between words which is known as CamelBack notation (Horridge et al., 2004).

The superclass Thing has RegulatorySource subclass that describes various types of regulatory documents for E-Government service development which is categorized in two disjoint subclasses. The InternalRegulation presents the regulations exist within the E-Government organization and ExternalRegulation presents the regulations from outside of the organization. The InternalRegulation has two subclasses, Policy Document presents the organizational own strategies of E-Government service development, AgreementDocument presents the contract information between the E-Government organization and other stakeholder involved in the E-Government service development. The ExternalRegulation has also two subclasses, Legal Document presents the local, national, and international level regulations where the E-Government system will operate, and StandardDocument presents the general guidelines and best practices of E-Government service development.

Furthermore, the Thing class has RegulatoryObjective subclass that describes the objectives of the E-Government regulations. The RegulatoryImpact class describes the overall abstract goals realized in the long run of the E-Government system operation. The RegulatoryOutcome class describes the immediate goal of the regulatory rules in the E-Government services. The Thing class has EgovService subclass that describes various types of services provided by the E-Government regulation. The G2C delivers E-Government services to the citizen, G2B delivers E-Government services to the business organization, and G2G delivers E-Government services to the employees of the public organization itself.

In Figure 17, the Thing class has RegulatoryRequirement subclass that describes different types of requirements originated from RegulatorySource. The System Requirement class describes the properties of the E-Government system that is disjoint with the Development Requirement class that describes the requirements need to be followed by the project management team during the E-Government project development. SystemRequirement is also classified into Operational Requirement that defines the functionalities of the E-Government system and QualityRequirement that defines how the system will perform its functional requirements. The QualityRequirement class has enumerated classes such as Availability, Security requirements, etc. to define non-functional properties of the E-Government system.

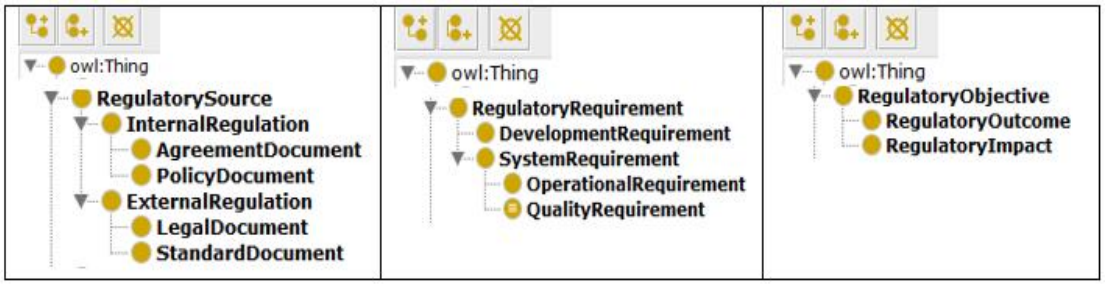


Figure 17: Class hierarchy of Regulatory Source, Requirement, and Objective

In figure 18, the Thing class also has a Stakeholder subclass that describes various types of participants in the E-Government system. Primarily there are three categories of participants in Stakeholder class. EgovDonor class partially or fully funds the E-Government projects, EgovUser class receives various types of E-Government services, and the ServiceProvider class provides resources and services to the E-Government system/users. The EgovDonor class is further classified in the Directorate, Division, and Unit of funding authority. EgovUser is classified into Citizen, Business organization, and Government employee. And, ServiceProvider class is classified into ITVendor who provides technical support to the E-Government system, GovAgency is another government organization that collaborates in providing one-stop E-Government services. The Thing class has RegulatoryRule subclass that describes various types of rules in the E-Government regulation. FactRule defines regulatory information about entities of the E-Government system. ActionRule defines the predefined actions in the system instigated by a regulation while a condition is met. ConstraintRule defines the restriction imposed by the regulations while performing system or user operation. And, ComputationRule defines the formula used in calculation by the E-Government system.

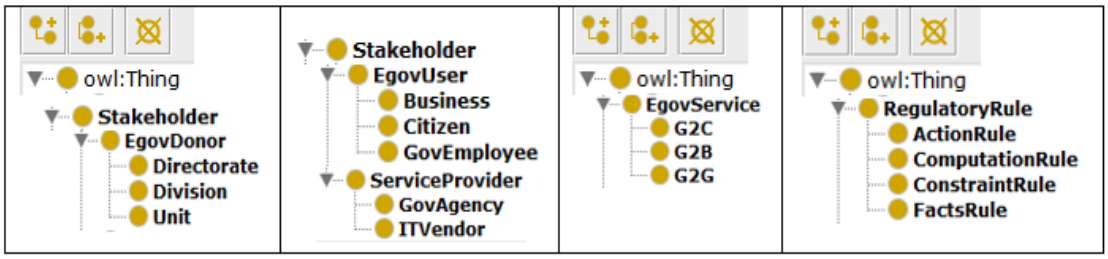


Figure 18: Class hierarchy of Stakeholder, E-Gov Services, and Regulatory Rules

Furthermore, in Figure 19, the Thing class has CompliancePriority subclass that describes the priority of regulatory requirements in the E-Government system. It has enumerated classes HighPriority that refers to complete compliance and the LowPriority class refers to optional compliance of the regulatory requirements in the E-Government system. The Thing class has ComplianceProbability subclass that describes the likelihood compliance of regulatory rules. It has TotalCompliance class that defines the compliance of every single principal in a rule and Partial Compliance class that defines the compliance of some part of a compound rule. The Thing class has RuleComplexity subclass that describes the complexity of a rule. It has SimpleRule class that defines a rule with a single directive, CompoundRule class that defines a set of rules combining with some logical operators. The Thing class has ComplianceImpact subclass that defines the consequence of regulatory non-compliance. It has SevereImpact class that defines costly penalties imposed by noncompliance of the regulatory rules, and NegligibleImpact class that defines no or negligible penalty for the noncompliance of the regulatory rules. The Thing class has RegulaotryAuthority subclass that describes the enforceability of rules in the E-Government system. It has Obligation class that defines the rule that is legally bound

to comply, and Privilege class that defines the opportunities that the E-Government system is permitted but not required to implement.

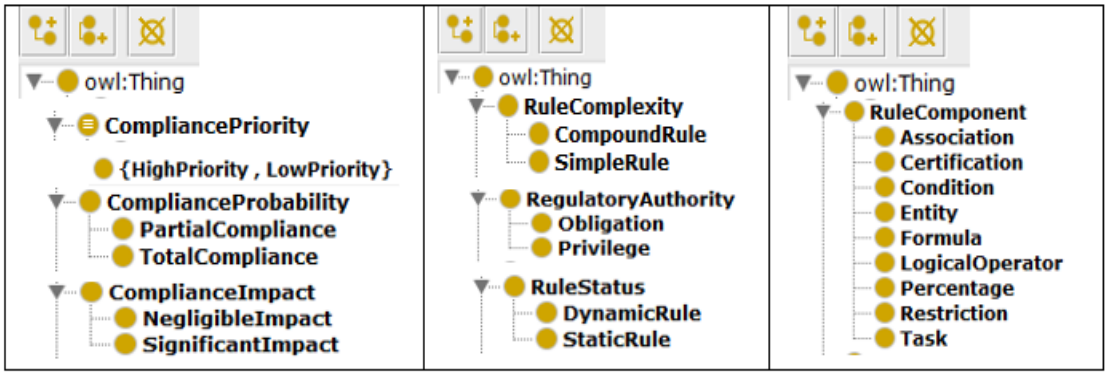


Figure 19: Class hierarchy of Regulatory Compliance, and Rule Components

The Thing class has RuleStatus subclass that describes the changing nature of the regulations. The DynamicRule class defines the regulations those are more subject to change and disjoint with the StaticRule class that defines the regulations those may not subject to any changes. The Thing class has RuleComponent subclass that describes various components in a rule. The Entity class describes various entities in the E-Government system, the Association class associates different entities in the rule. The Condition class presents various conditions in the E-Government system operation. The Formula class presents various methods for calculation. The LogicalOperator class combines the sub parts of a rule. The Restriction class presents various constraints in operating an E-Government system. The Task class presents the works to be performed according to the regulation. The Percentage class defines various percentages in the formulation of a regulatory rule. The Certification class defines a list of certificates of the system operations to comply with the E-Government system.

3.5 Class Properties of EGRRC Ontology

The class properties represent relationships among various classes or individuals. Although, there are no strict rules for naming object properties in protégé, however, it is recommended to name the object properties starting with a lower-case letter and remaining capitalized words with no space in between.

Figure 20 presents the property hasAffect that describes the affected EgovService by the RegulatorySource, hasGoal describes the RegulatoryObjective added by the RegulatorySource, and isSourceOf describes the RegulatoryRequirement from the RegulatorySource. The property isInternalSourceOf explains the RegulatoryRequirement originated from inside of the E-Government service development organization. The hasOrgRegulationOf describes EgovService from various policies existing in the organization where the E-Government service is being developed. The hasContractualRegulationOf describes the agreements made in

EgovService, the hasAgreementWith describes relationships between Agreement Document with various types of the Stakeholder in the E-Government service development. The agreementValidity defines the validity period of conditions presented in the AgreementDocument which may renegotiate after the Restriction of time constraint. The hasResult explains the relationship between Regulatory Source with RuleStatus. The regulations presented in InternalRegulation are the DynamicRule where the E-Government organization are directly involved in creation and amendment of regulation over some period when necessary and agreement Validity has ended. The isExternalSourceOf explains the RegulatoryRequirement originated from outside of the E-Government organization. The regulations presented in ExternalRegulation are the StaticRule where the E-Government organizations are not directly involved in the creation and amendment of regulations. The External Regulations are the source of QualityRequirement as the regulations presented in these documents are mainly describing the non-functional properties of the E-Government system. The LegalDocument presents the authoritative regulations and StandardDocument presents the best practice of EgovService.

Figure 20: Class properties of Regulatory Sources

Figure 21 presents the isGoalOf property describes the origins of Regulatory Objective from RegulatorySource, and hasLongTermGoal and hasShortTerm Goal properties define the long-term abstract goal and short-term immediate goal of the RegulatoryRequirements in the E-Government service development. The RegulatoryImpact class that describes the long-term abstract goal of E-Government service development isGoalOf the AgreementDocument and particularly made with EgovDonor of the Stakeholder class who funds the E-Government projects. On the other hand, the RegulatoryOutcome class that describes the immediate goal of regulatory objective isGoalOf mainly the InternalRegulation in the organization.

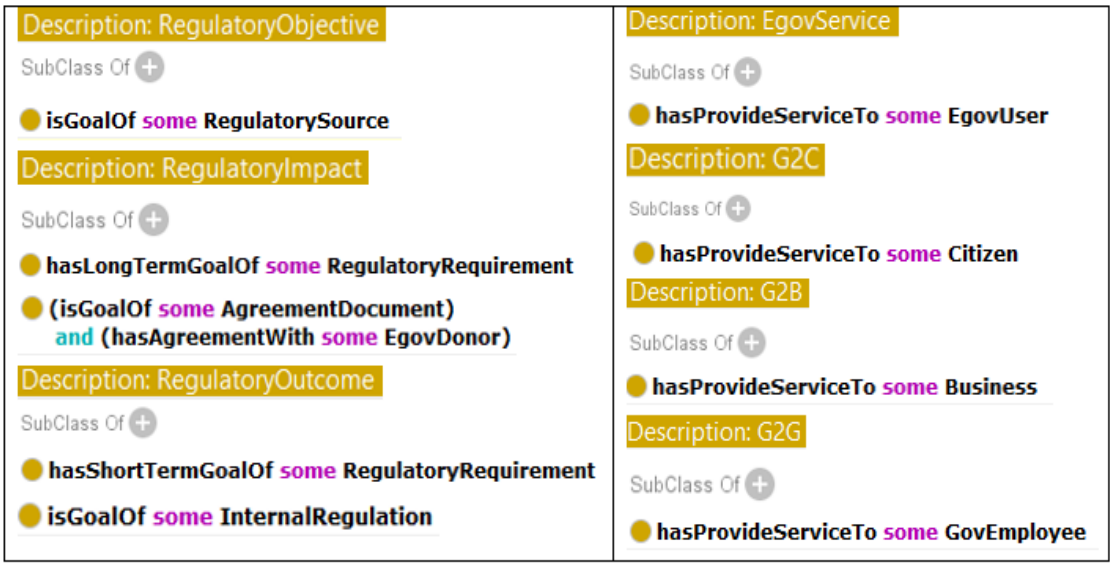


Figure 21: Class properties of Regulatory Objectives and E-Gov Services

The hasProvide ServiceTo property describes the E-Government service delivery to various EgovUser groups in the Stakeholder class as different types of users need different types of services from the E-Government system. A G2C system provides e-services to the citizens of the E-Government user groups. A G2B system provides E-Government services to the business organization. And, a G2G system serves the employees of the public organizations.

Figure 22 presents the property isOriginatedFrom that describes various types of RegulatoryRequirements from the RegulatorySource. The SystemRequirement is originated from all types of RegulatoryDocuments whereas the Agreement Document and PolicyDocument are mainly source of the Development Requirements in the E-Government project development.

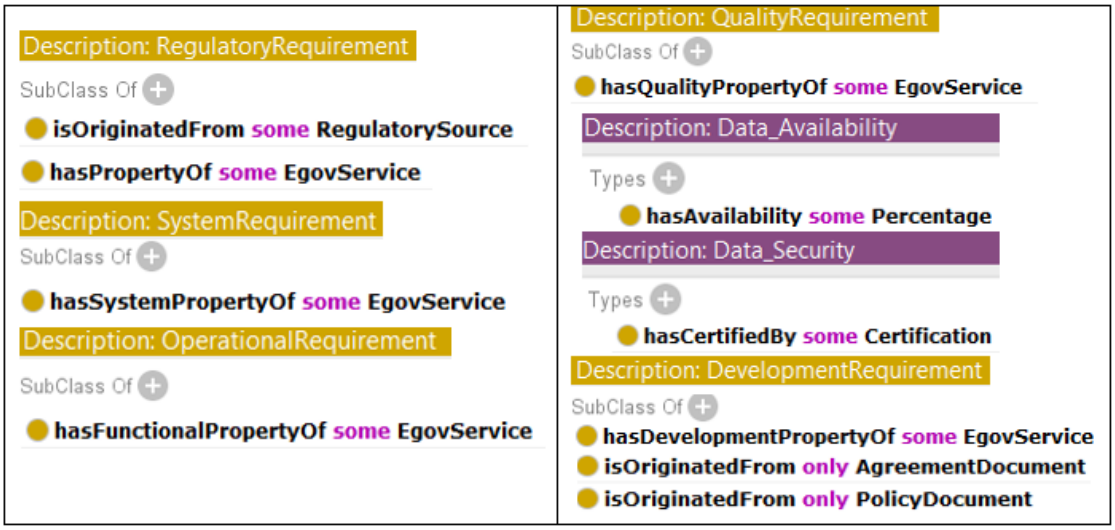


Figure 22: Class properties of Regulatory Requirement

Furthermore, the hasDevelopmentPropertyOf describes the Development Requirement, and hasSystemPropertyOf describes the types of System Requirement, hasFunctionalPropertyOf describes the OperationalRequirement, and hasQualityPropertyOf describes the non-functional attributes of the Quality Requirement in the E-Government services. In the enumerated class of Quality Requirement, the property hasAvailability describes the percentage of Availability of an E-Government service to its users. The property hasCertifiedBy describes the list of certifications to ensure the Security of an E-Government system.

In Figure 23, the Stakeholder class presents the property hasFund that describes who funds about what Percentage in the E-Government service development project in case if there are multiple Donors in the project initiatives. Furthermore, the hasReceive class property describes the EgovService requested and received by various EgovUser. The hasProvideSupportTo describes the EgovService supported by various types of ServiceProvider in the E-Government system, the ITVendor provides technical support and GovAgency provides collaborative support to the E-Government system development.

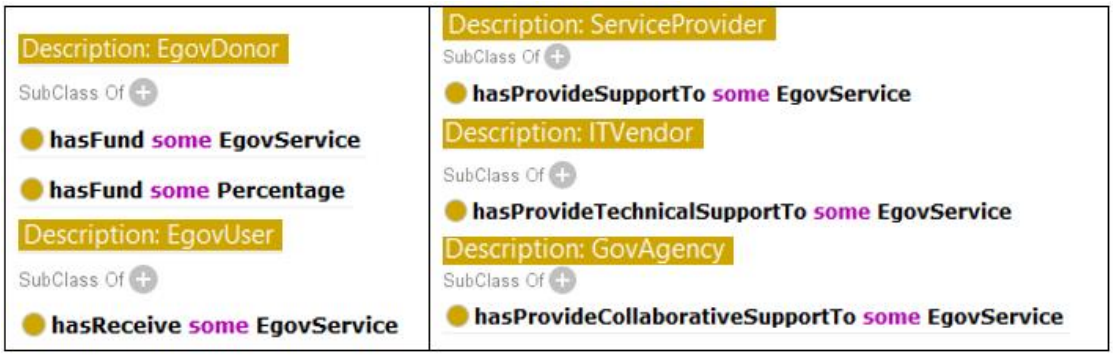


Figure 23: Class properties of E-Government Stakeholder

Figure 24 presents the RegulatoryRequirement that has been produced by various kinds of RegulatoryRules such as action rules, fact rules, constraint rules, computation rules, etc. The ActionRule has relationships with Stakeholder class, Task and Condition sub-class of the RuleComponent class through the properties hasAllow, hasPerform, and isBasedOn respectively. Action rules describe the triggering event of an action to be performed in the system operations. Furthermore, the ActionRule essentially allows various Stakeholder roles in the E-Government system to perform some tasks based on some Conditions written in the regulation. The FactRule describes the relationships between various important individuals of Entity class with the Association class through the object properties hasRelation Between and isBasedOn in describing meaningful information and data model in the E-Government system domain. It basically generates some association between some important entities in the E-Government system. The ConstraintRule has also relationships with the Stakeholder class as well as the Task, and Restriction sub-class of RuleComponent class through the object properties hasAllow, has

Perform, and isBasedOn respectively. It largely allows some Stakeholder roles in the E-Government system to perform some tasks based on some restrictions written in the regulations. And finally, the ComputationRule describes some Tasks to be performed in the E-Government system operation based on some predefined Formula or algorithms to solve a particular problem or calculate some data to produce results and information.

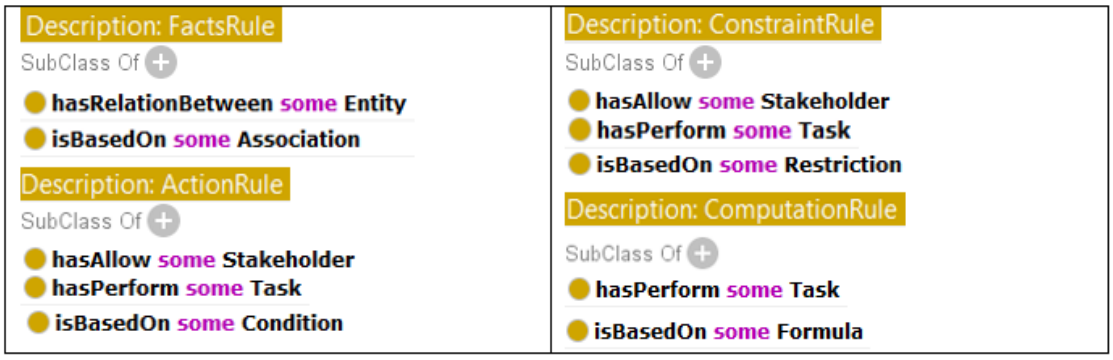


Figure 24: Class properties of Regulatory Rules

In Figure 25, the CompliancePriority class describes the priority of regulatory requirements in the E-Government system through the relationship between ComplianceProbability class and ComplianceImpact class. The class property hasProbabilityOf explains the probability of non-compliance and hasSeverityOf explains the impact of non-compliance. The HighPriority of regulatory compliance hasProbability of TotalCompliance and hasSeverityof substantial level of SignificantImpact. The LowPriority of regulatory compliance hasProbabilityOf the PartialCompliance and hasSeverityOf insignificant level of NegligibleImpact.

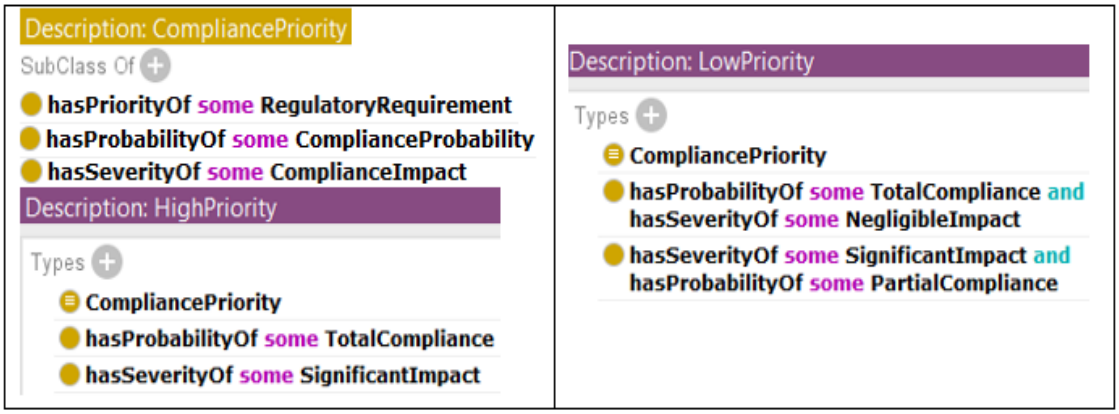


Figure 25: Class properties of Compliance Priority

Furthermore, in Figure 26 & 27, the TotalCompliance of regulatory rules is considered when the regulatory rule hasCoverWholeOf the SimpleRule which does not have any LogicalOperator. And, the SignificantImpact class has mandatory compliance of the Obligation rule which should be satisfied fully in the E-Government system development. The PartialCompliance of the regulatory rule

hasCoverPartOf a CompoundRule which has at least one LogicalOperator that combines multiple principles or clauses.

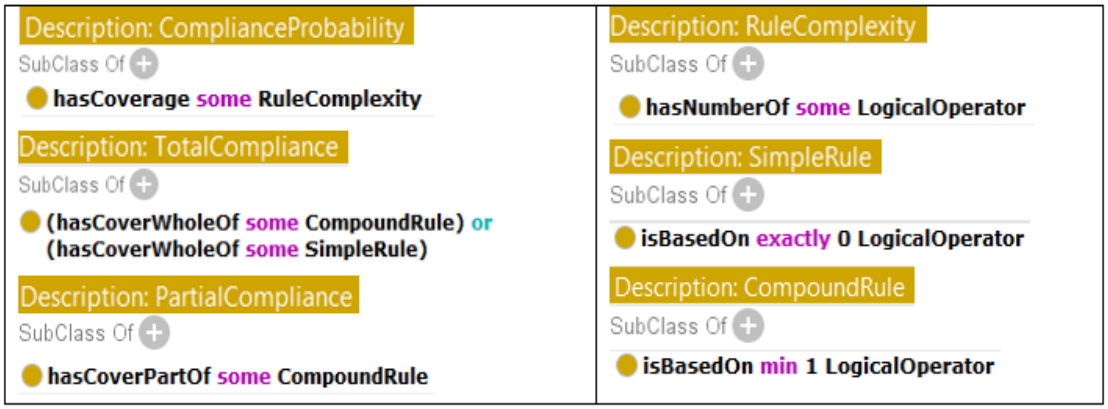


Figure 26: Class properties of Compliance Probability and Rule Complexity

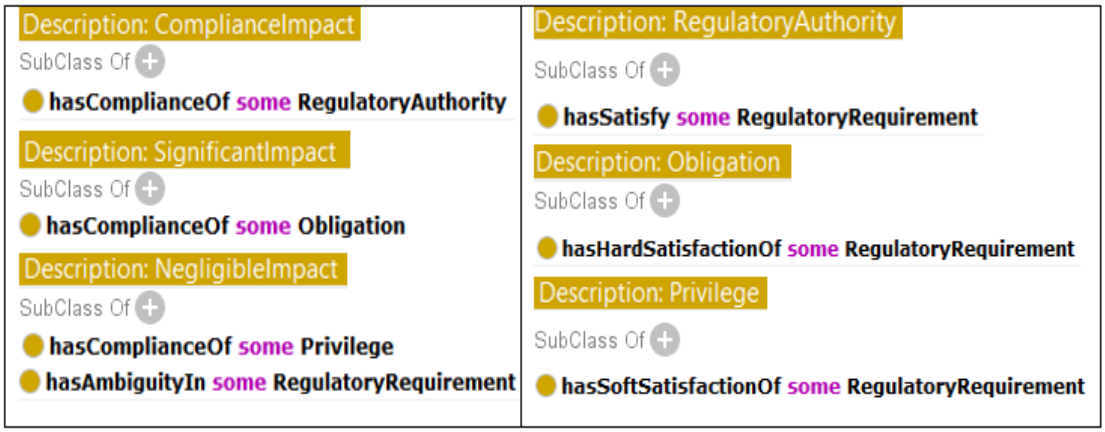


Figure 27: Class properties of Compliance Impact and Regulatory Authority

Figure 28 presents the isOriginatedFrom property describes the StaticRule that mainly comes from LegalDocument and StandardDocument where there is little scope of ambiguous RegulatoryRule. On the other hand, the DynamicRule mainly comes from the organization's AgreementDocument and PolicyDocument which are more vulnerable to the ambiguous regulations and there is room for possible regulation amendment.

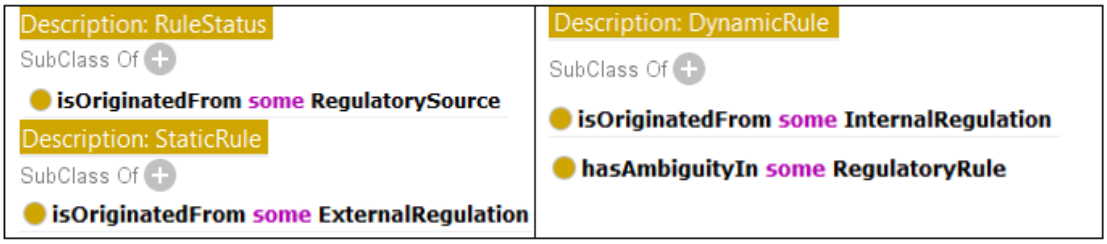


Figure 28: Class properties of Regulatory Rule Status

Figure 29 presents the concepts of the E-Government Regulatory Requirements Compliance ontology (EGRRC) showing the interrelationships between the classes in the class hierarchy through various class properties.

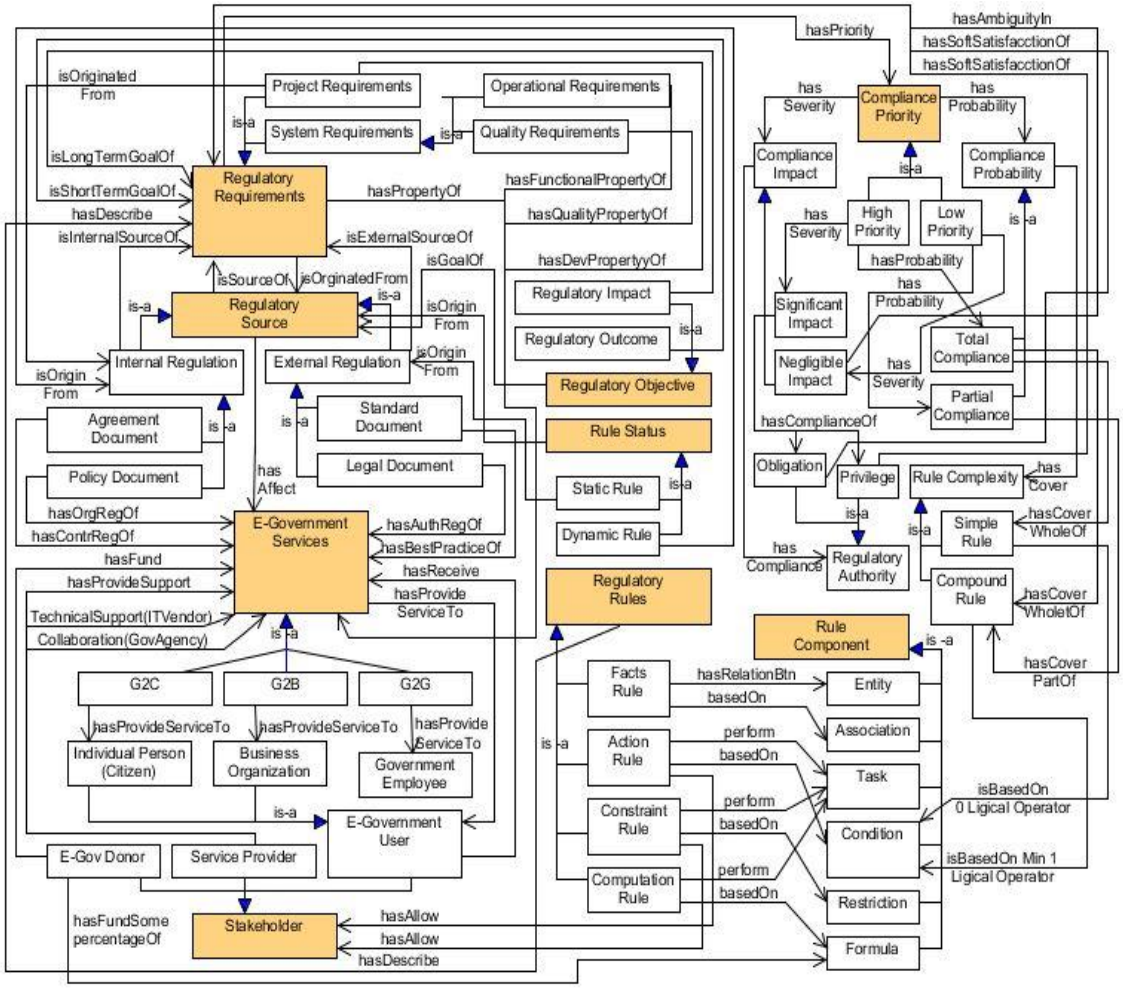


Figure 29: E-Gov Regulatory Requirements Compliance Ontology (EGRRC)

3.6 Evaluation of EGRRC Ontology with GDPR case

The General Data Protection Regulation (GDPR) is implemented in the proposed EGRRC ontology. The European Commission has presented the new GDPR regulation which is planned to replace the old Directive 95/46/EC 1995. The GDPR constitutes the legal framework for personal data processing in EU countries. The GDPR is presented not only to harmonize data privacy laws across Europe in protecting the rights of using individual's personal data but also to facilitate the freedom of exchanging personal data within member states of European Union through a uniform legislation towards advancing the digital agenda and economic growth across EU countries (Nyren et al., 2014; Voss, 2014).

The GDPR has enacted on 25 May 2018 to all the member counties under the European Union (EU) as well as the organizations from outside of the EU zone operating in the EU countries should comply with the regulation. Given the conditions in the GDPR to work with large volumes of data which may contain sensitive personal information of the citizens and business organizations, the GDPR compliance should be the key priority to the local and central governments of EU countries who process this personal information. The negligence of the newly enacted GDPR in the data processing operations has serious implications both monetary as well as reputational. This could be extremely costly for the data processing organizations given the fines up to €20 million or 4 percent of the global revenue and on top of losing the reputation and citizen trust on the government regarding their personal information. In case of the previously enacted regulations, the non-compliance of the regulatory requirements would charge the data processing organizations with relatively a very small amount of monetary fine compared to the newly enacted GDPR regulation. The GDPR introduces new requirements on how to collect, process, store, and transfer personal data where there is lots of fear, uncertainty and doubt to understand many complex aspects of the regulation on how it affects in the system operation said by Andrew Burt, the chief privacy officer and legal engineer at the Immuta, an information governance platform (Anadiotis, 2018).

In this section, the evaluation of the proposed EGRRC ontology and its suitability in ascertaining the research objectives have been discussed. The concepts classes and their interrelationships defined in the EGRRC ontology are validated in the following two ways of systematic ontology evaluation process. First the EGRRC ontology has been validated in respect to the quality assessment criteria and then the usefulness of the EGRRC ontology has been validated by demonstrating the results of the queries made in the ontology.

The instantiation of the concepts regarding personal data processing found in the GDPR and mapping these concepts into the entities of the EGRRC ontology may help the involved system development stakeholder to understand how the newly introduced legislation affects in the E-Government system development in EU countries and what actions or documents are needed from their side as part of their positioning in the operational chain. Furthermore, the citizens and business organizations, the owner of the data will have more clear understanding of their rights and control over the personal data they have provided to the data processor, the government agencies in EU counties. The purpose of the EGRRC ontology is not to completely describe the concepts of the frameworks such as GDPR but to demonstrate their influence and provide the aforementioned guidance to the involved stakeholder working with GDPR. The IT professional of the data processing organizations can use the EGRRC ontology framework in their daily works while mapping the concepts from newly enacted GDPR to the defined entities of EGRRC ontology in order to clearly understand their actions of dealing with personal information.

3.6.1 Quality Assessment of EGRRC Ontology

There are six evaluation criteria presented by Gruber (1995) which has been widely used in many works on ontology development later on to evaluate the quality of an ontology (Pak & Zhou, 2009; Sarantis & Askounis, 2009; Milton et al., 2012; Wand et al.,1999). These six evaluation criteria are explained and considered in this study to validate the quality aspect of the proposed ontology. Based on the quality assessment criteria presented by Gruber (1995), the EGRRC ontology has been assessed in terms of consistency, completeness, conciseness, clarity, generality, and robustness of the ontology description.

(A) Consistency of the EGRRC Ontology Description

Consistency of the ontology description refers to the absence of contradictory information regarding the class definition and their relationships. For example, the ontology has semantic consistency in the formal and informal definitions created and inferred in the ontology. One of the key features of building ontologies using protégé is that the ontologies can be processed by a reasoner to check the consistencies of all definitions created and inferred knowledge in the ontology description. In order to validate the consistencies of the ontology descriptions, the EGRRC ontology is executed using the FaCT++ tableaux-based reasoner that comes with protégé ontology development tool to verify the Description Logics (DL). The FaCT++ reasoner is applied in the EGRRC ontology to verify and ascertain the default tableau rules such as conjunction, disjunction, existential quantification, value restriction, negation, clash rules. It automatically computes the class hierarchy into the inferred hierarchy to automatically verify the ontology and check the logical consistency of the ontology description. If a class is found to be inconsistent with its descriptions and relations with other classes, the name of the class will be highlighted in red color for its inconsistencies. For example, if an individual is instantiated into two different classes in the ontology and these two classes are disjoint with each other in this case the FaCT++ reasoner will give an inconsistency error since the individual cannot be an instance of both classes. The execution of the FaCT++ reasoner verifies the EGRRC ontology with no inconsistencies in its definitions.

(B) Completeness of the EGRRC Ontology Description

Completeness of the ontology description refers to the lack of incompleteness in the ontology descriptions and how well the ontology covers the real-world scenario of the E-Government project management. An ontology is considered to be complete if all the information related to the domain knowledge is explicitly defined in it or can be inferred from the other definition. Sometimes some important concepts of an ontology can be overlooked in the definition and this incompleteness of information often leads to ambiguity while mapping the ontology in the real-world scenario. To detect the incomplete descriptions of EGRRC ontology, the class hierarchy, domain, and scope of the relationships in the ontology are verified with a case study of the General Data

Protection Regulation (GDPR). The instantiations of the concepts found in GDPR have been completely mapped into the entities of the EGRRC ontology in order to create the framework's description in E-Government system development.

Furthermore, one of the most powerful features of OWL ontology is the inference that reasons with the ontology elements and infer knowledge to make explicit what is implicit in the ontology. The inference finds some of the implicit relations based on the explicit definition of the ontology to complete the descriptions. For example, the StaticRule class has also disjoint with DevelopmentRequirement class along with DynamicRule class. The LegalDocument and StandardDocument classes are disjoint with the InternalRegulation class. The PolicyDocument and Agreement Document classes are also disjoint with ExternalRegulation class. The Compound Rule class is disjoint with SimpleRule class based on the explanation shown in the Figure 30 and 31.

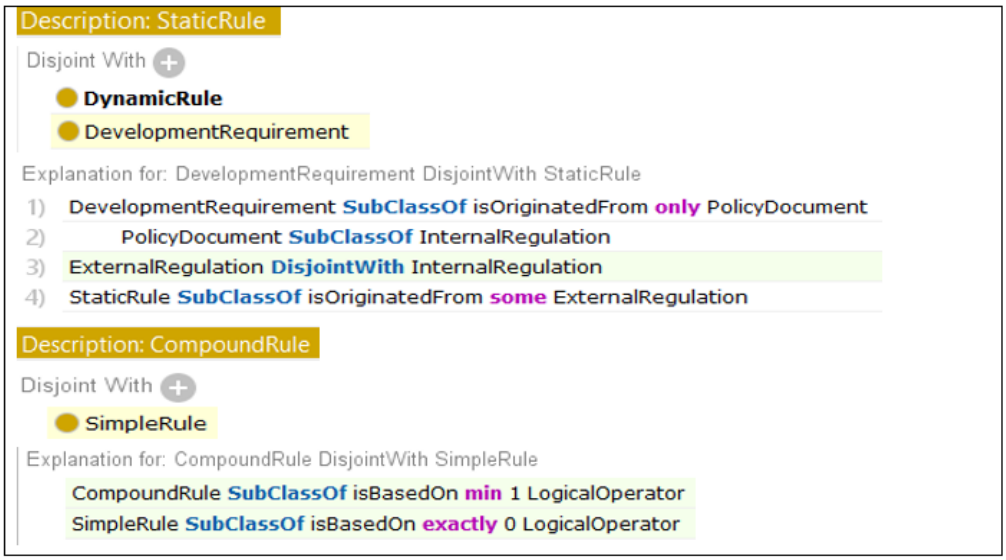


Figure 30: Inference properties found in Static and Compound rule

Figure 31: Inference properties found in Legal Docs and Operational Req

(C) Conciseness of the EGRRC Ontology Description

Conciseness of the ontology description refers to the absence of unnecessary and irrelevant information defined in the scope of the ontology description. It also implies the absence of redundant representations of the concepts defined in the ontology descriptions. In order to evaluate the conciseness of the EGRRC ontology, the instantiation of the concepts found in GDPR have been mapped into the entities of the EGRRC ontology. The intend of the instantiation from GDPR case is to reflect if the EGRRC ontology defines irrelevant elements with regards to the scope of the E-Government regulatory requirements compliance domain (e.g., ontology elements that cannot have any instances) or if there is any redundant representation of the elements in the ontology description (e.g., single instance can be used in multiple elements of the ontology description). The GDPR instantiation in EGRRC has left no ontology elements to be unused for creating individual instances in the class hierarchy. And, no such instances of a class are used in other places of the class hierarchy with the redundant description of the ontology elements.

(D) Clarity of the EGRRC Ontology Description

The clarity of the ontology description refers to the meaningful semantics of the classes in the ontology class hierarchy and the relationships between the classes. The ontological clarity defines how clearly the ontology model represents the semantics of the domain and how effectively the intended meaning is communicated through the ontology description.

The clarity of EGRRC ontology description signifies to provide precise meaning of the ontology elements to reduce the semantic ambiguity by avoiding construct overloading, construct redundancy, and construct excess. When the instances of construct overloading, redundancy, and excess exist in the definition of any ontology elements, the meaning of the ontology constructs will be unclear. The construct overloading in EGRRC ontology description is evaluated if a single instance extracted from the GDPR regulation text maps into two or more elements in the ontology class hierarchy. The construct redundancy is evaluated if two or more redundant instances from the GDPR text map to a single EGRRC ontology element. And finally, construct excess is evaluated if any instance does not map onto any of the ontology elements described in the class hierarchy.

The evaluation of construct overloading, redundancy, and excess by the mapping of instances from GDPR regulation text into EGRRC ontology description confirms that there are one-to-one relationships between the instances from GDPR and EGRRC ontology elements where any instance does not belong to multiple ontology elements nor many redundant instances are mapped to a single ontology element. Also, the evaluation confirms that every instance extracted from the GDPR regulation texts can be mapped in the EGRRC ontology elements.

(E) Generality of the EGRRC Ontology Description

The generality of the ontology description refers to the reusability of the ontology elements for various purposes within the domain area of E-Government project management. The reusable ontology provides an unambiguous basic set of vocabulary which can be shared by some other process or application development within the application domain. The EGRRC ontology is developed based on the already established vocabulary from existing ontologies in various scope of the E-Government domain. For example, the elements of the EGRRC ontology are reused from E-Government project monitoring and management ontology, E-Government service quality ontology, E-Government process ontology, E-Government goal ontology, etc. Therefore, the proposed EGRRC ontology can be easily reusable and adaptable in the various other scope of the E-Government information system development project domain.

Another indication of the generality of the EGRRC ontology is that it defines the kind of or type of relationships among superclass and subclass in a class hierarchy. The classes which cannot be instantiated by any instances are essentially not a general class in the ontology. The general classes in the ontology always have instances to specify the general description of the class hierarchy. In the EGRRC ontology the general class has top-down breakdowns among different levels of classes in the hierarchy and every class in the class hierarchy may have instances to specify the class descriptions.

(F) Robustness of the EGRRC Ontology Description

Robustness of the ontology description refers to the modification capability of the ontology for any further change required. It represents the sensitivity of the definitions that exists in the ontology. If a small change in the class definitions is performed, then it will alter the other definitions related to that class definition. The robustness of EGRRC ontology is evaluated regarding the sensitivity of the defined ontology entities towards adapting change in the ontology descriptions. For example, if the DevelopmentRequirements subclass of RegulatoryRequirements class needs to have some further breakdown of BudgetConstraint of project expenditure, TimeConstraint of project deliverable deadlines, ResourceConstraint of project management human resource and tools to be employed in the project, then these subclasses of the DevelopmentRequirements by default adopt the relationships of isOriginatedFrom the PolicyDocument and AgreementDocument, as well as the hasDevelopmentPropertyOf the EgovServices in the E-Government system development from their superclass. Also, these newly created classes are disjoint with the SystemRequirement and StaticRule class. Therefore, if the EGRRC ontology does not have robustness regarding the sensitivity of the ontology description, then any modification would not have any affect in the ontology description.

3.6.2 Usefulness Assessment of EGRRC Ontology

One of the main objectives of the ontology development is to represent the interconnected knowledge of the ontology become useful in the E-Government project development in answering their queries. The ontology usefulness validation process involves taking an ontology of defined concepts and a set of documented texts describing a particular domain such as GDPR regulations. The documents are then used in populating the ontology instances from the texts to identify if the ontology returns correct/incorrect instances refereeing in the texts regarding the particular queries made in the ontology. For example, the ontology returns an incorrect value of £2000 as belonging to the concepts of skills class instead of salary class (Gómez-Pérez, 1995; Hartmann et al., 2004).

The usefulness evaluation of the EGRRC ontology has been made by implementing the newly enacted GDPR regulation into the proposed EGRRC ontology. There are total 82 instantiations of the concepts found in GDPR have been mapped to the defined entities of the EGRRC and CISMET ontology in order to create the framework's description. The instantiation process of extracting individuals from the GDPR text has been presented in Appendix-I. Furthermore, the DLquery functions of the protégé tool has also been used in this study to present relevant queries and their results. DLquery is a powerful and easy-to-use OWL query language feature in the protégé for searching classified ontologies. DLquery provides an interface in the protégé tool to write queries and get the results of the queries. To run the queries in the DLquery interface the ontology has been classified by a reasoner such as FaCT++ reasoner. The query statements have been built using the class expression defined in the ontology which describes the class properties following the object classes explained in the ontology triple descriptions. Furthermore, DLquery allows the users to combine multiple queries using AND/OR operator to get their integrated results (e.g., intersection or common instances of multiple class expression or queries).

This can aid the involved stakeholders to understand how the newly introduced GDPR legislation affects them and what actions or documents are needed from their side as part of their positioning in the operational chain. For example, identify the existing internal and external laws, policies and agreements made with various stakeholders in the GDPR regulation and the validity period of the regulations in the E-Government system development. Also, identify the defined long-term and immediate goals of the E-Government system development found in the GDPR regulation. Identify and understand the effects of the GDPR regulations on various services provided by the E-Government system. Identify the constraint or restriction rules for the system development, functional, and quality properties of the E-Government system and its operations. Identify and understand the high prioritized obligatory rules and low prioritized optional rules in the E-Government system development. Also, identify the stability of the rules and potential future amendments of the dynamic regulatory rules in the GDPR regulation to be compliant in the E-Government system.

In Figure 32-34, the following queries (along with their results) are presented:

- What are the regulatory documents referenced in GDPR that are internal and external sources of regulatory requirements with static and dynamic rules?
- What are the regulatory documents that have agreement with the data controller and agreement length is 3 years to revise the conditions of the regulation if necessary?

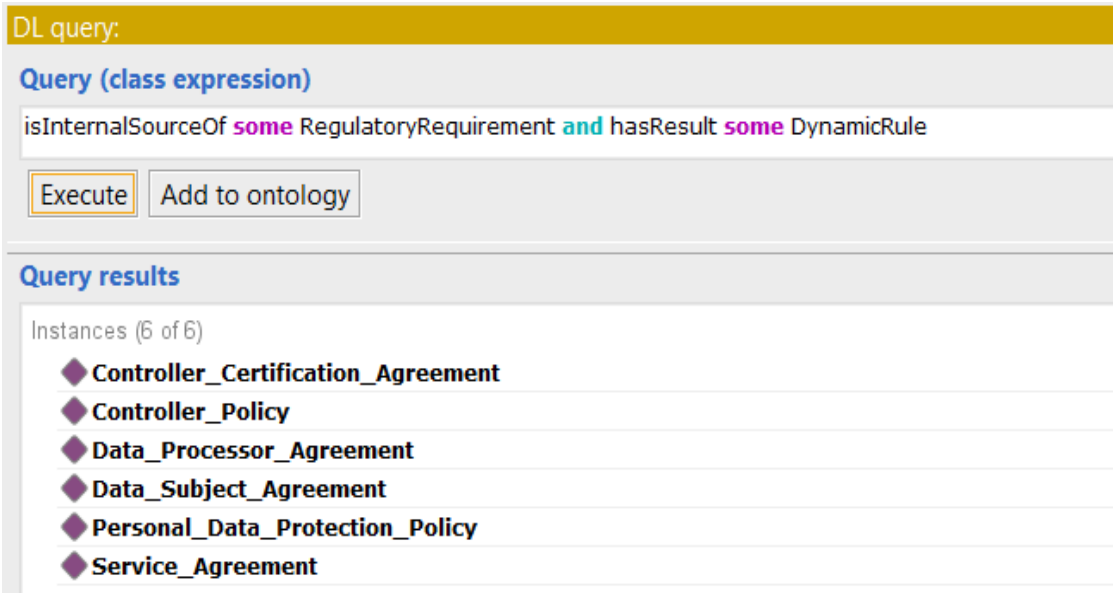


Figure 32: Internal source of regulatory requirements in GDPR

Figure 32 presents the query results of the internal source of regulatory requirements. In GDPR, there are several internal sources of regulatory requirements such as various policy and agreement documents. For example, the Policy Documents are the Controller Policy that defines the controller's responsibility assignment, training in data processing and related audits, Personal Data Protection Policy followed by the data processing organization of one country in transferring data to other controller or enterprises in third countries. The Agreement Documents are the Data Subject Agreement that defines the contract between the data subject and the data controller for giving consent related to the data processing. The Data Processor Agreement defines the contract between data the controller and the data processor in carrying out of data processing tasks by a processor, Service Agreement defines the service contract for fulfilling the tasks of data protection officers other than the staff member of controller or processor, the Controller Certification Agreement defines the contract between the controller and the supervisory authority in the data processing.

Figure 33 presents the query results of the external source of regulatory requirements. There are several external sources of regulatory requirement documents are referenced in the GDPR regulations such as various legal and standard documents. For example, the Legal Documents are the Union Law that defines the regulations operating within the EU countries such as the GDPR that provides the legal framework for processing personal data across the EU member states.

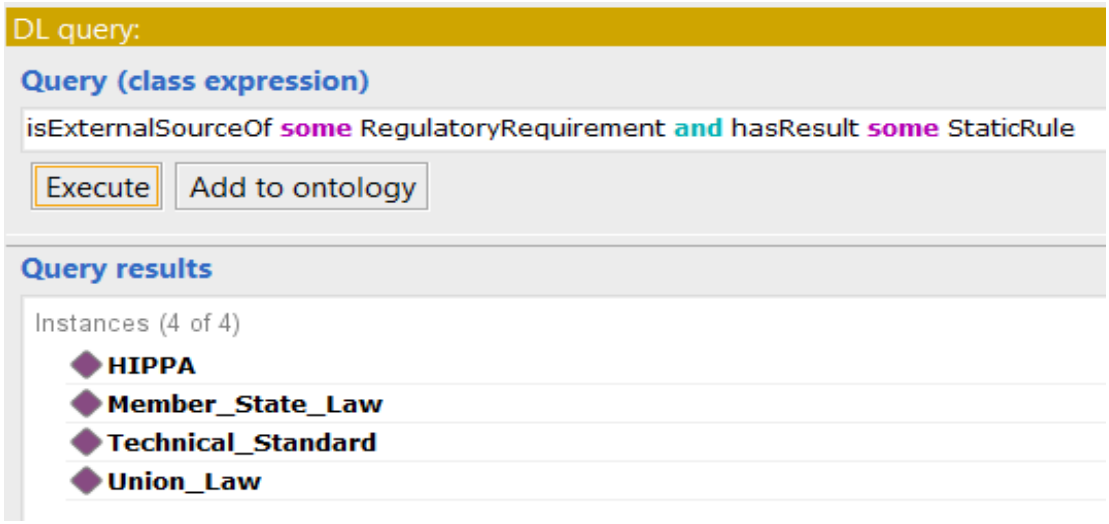


Figure 33: External source of regulatory requirements in GDPR

The Member State Law defines the national level and regional level regulations where each member state under the EU directives has its own law and legal system. The national regulations are valid anywhere in the state and the regional regulations are only applicable in certain areas, regions, or cities of the state. The Standard Documents are the Technical Standard that defines recognizable certification mechanism of data protection seals and marks in providing certificates to the data processor, the HIPPA defines the Health Insurance Portability and Accountability Act (referenced in the GDPR) as general guidelines for the electronic exchange, privacy, and security of the health information.

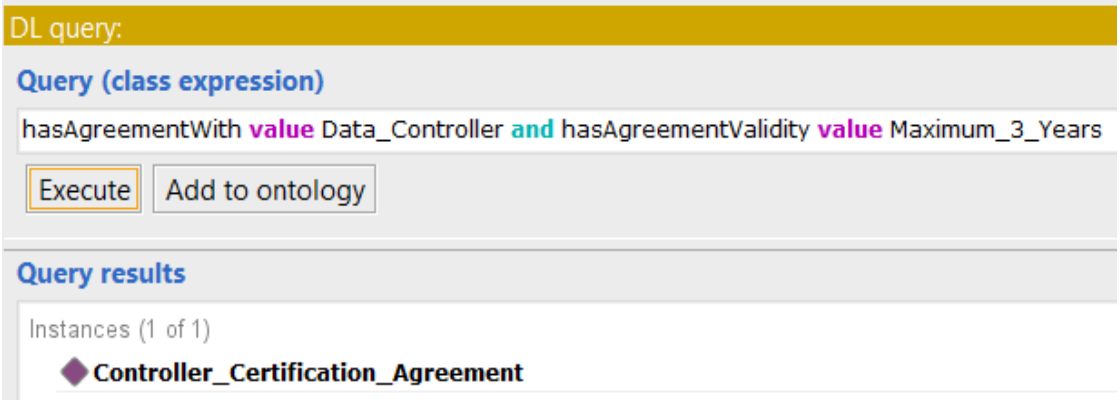


Figure 34: Agreements made with data controller for three years

Figure 34 presents the query results of the agreements made with the data controller in the GDPR regulation. The Controller Certification Agreement defines the contract between the data controller with the supervisory authority who monitors the compliance of the GDPR and issues certificates of data processing for a period of three years of renewable contract length.

In Figure 35 and 36, the following queries (along with their results) are presented:

- What regulatory requirements have long term abstract goals and short-term immediate goals in a system development referenced in the GDPR regulation?

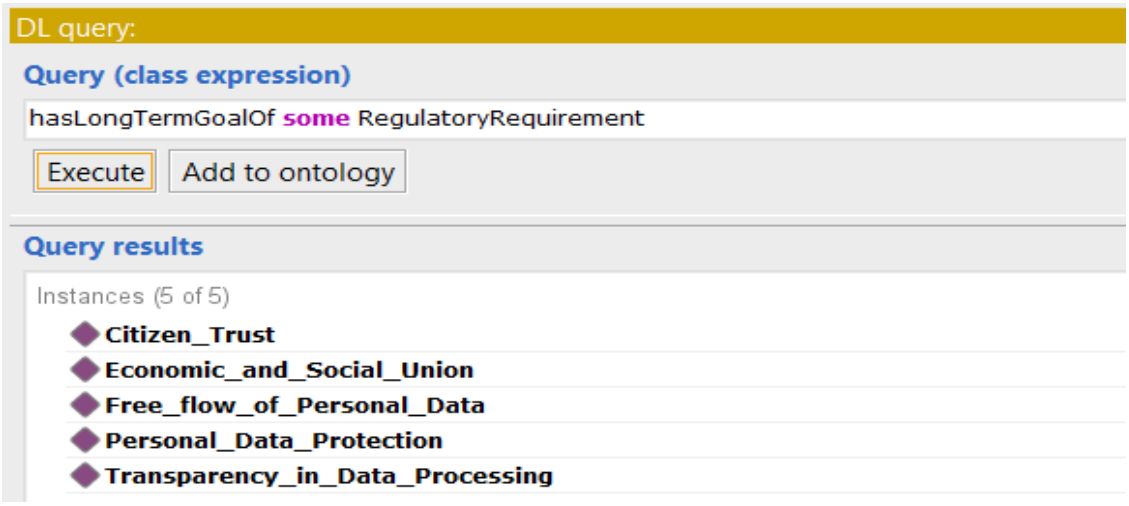


Figure 35: Long Term Goal of Regulatory Requirements in GDPR

Figure 35 presents the long-term abstract goals referenced in GDPR regulation are the Personal Data Protection that defines the goal of safeguarding the rights of the data subject in processing their personal data, Free flow of Personal Data defines the goal of information sharing among the member states and third countries without violating the rights of the data subject, Economic and Social Union defines the goal of strengthening the economic market by cross-border flows of personal data. The GDPR also has the goal to establish Transparency in Data Processing and achieve Citizen Trust in processing their personal data over electronic media.

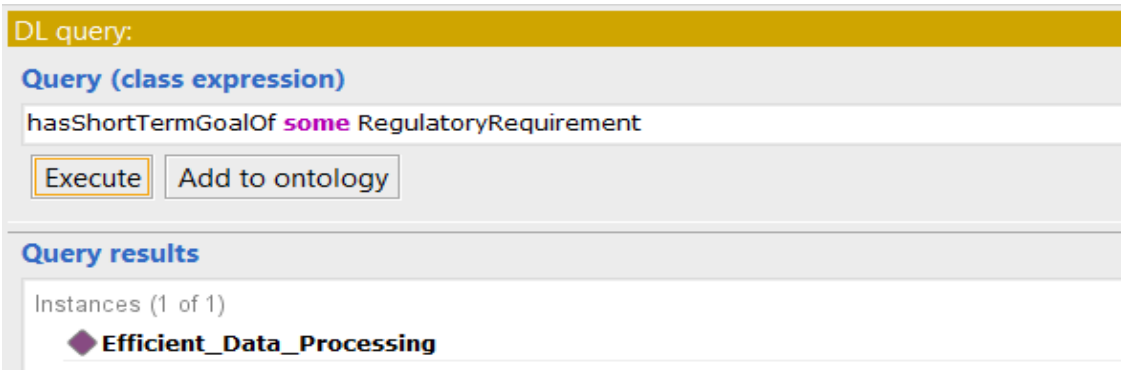


Figure 36: Short Term Goals of Regulatory Requirements in GDPR

Figure 36 presents the short-term immediate system development goals referenced in GDPR regulation are the Efficient Data Processing that defines the immediate goal of automated processing of personal data in filing systems which are accessible according to specific criteria (relating to whether the data are located in centralized, decentralized or dispersed on a functional or geographical basis).

In Figure 37-40, the following queries (along with their results) are presented:

- What services are affected by the new enacted GDPR regulation that provide electronic services to the business organization or government agencies of EU member countries?
- What regulatory requirements in GDPR have system development properties?
- What regulatory requirements in the GDPR regulation have functional properties and quality properties of an electronic system?

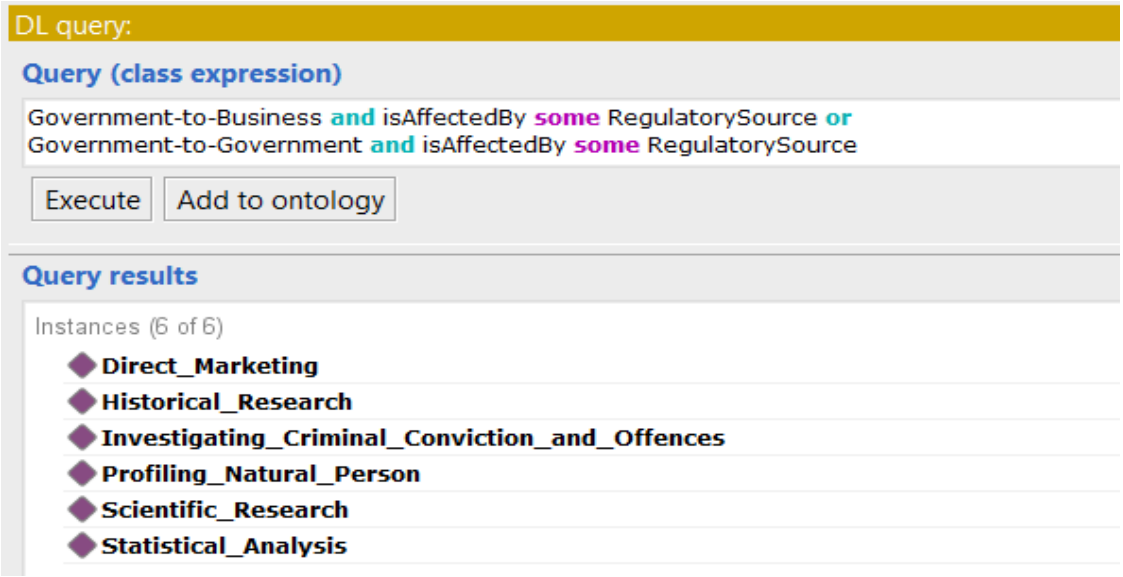


Figure 37: G2B and G2G services that affected by GDPR regulation

Figure 37 presents the Government-to-Business (G2B) services and Government-to-Government (G2G) services. The GDPR regulation has effects on three types of E-Government services (G2G, G2B, G2C). In G2B service, personal data are used for Direct Marketing purposes, Profiling Natural Person in monitoring the data subject's performance at work, economic and health situation, interest, reliability, and behavior in decision making. In G2G service, the personal data are processed in Investigating Criminal Conviction and Offences in measuring the threats to public security, Scientific Research, Historical Research, and Statistical Analysis purposes of public interest. Furthermore, in G2C service, the Health Care System provides information requested by the citizens about their medical treatment history and clinical treatment from the hospital.

Furthermore, Figure 38 presents the query results of The project development requirements of GDPR regulation are the Collaboration that defines the cooperation between the data controller, data processor, and supervisory authorities of member states in processing personal data, Testing and Monitoring defines the process of regular assessment and evaluation of the technical and organizational effectiveness measures for ensuring the security of data processing, Training defines the data protection awareness raising and staff training involved in data processing.

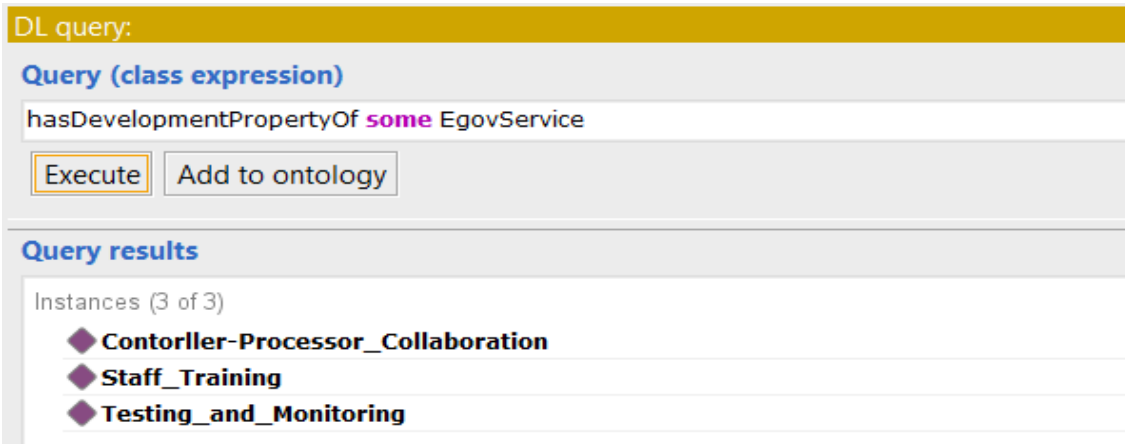


Figure 38: Project Development Requirements from GDPR

Figure 39 presents the query results of the system operational requirements referenced in GDPR regulation are the Data Collection, Data Storing, Data Processing, Data Access, and Data Transaction that define the functionality of the E-Government system with personal data.

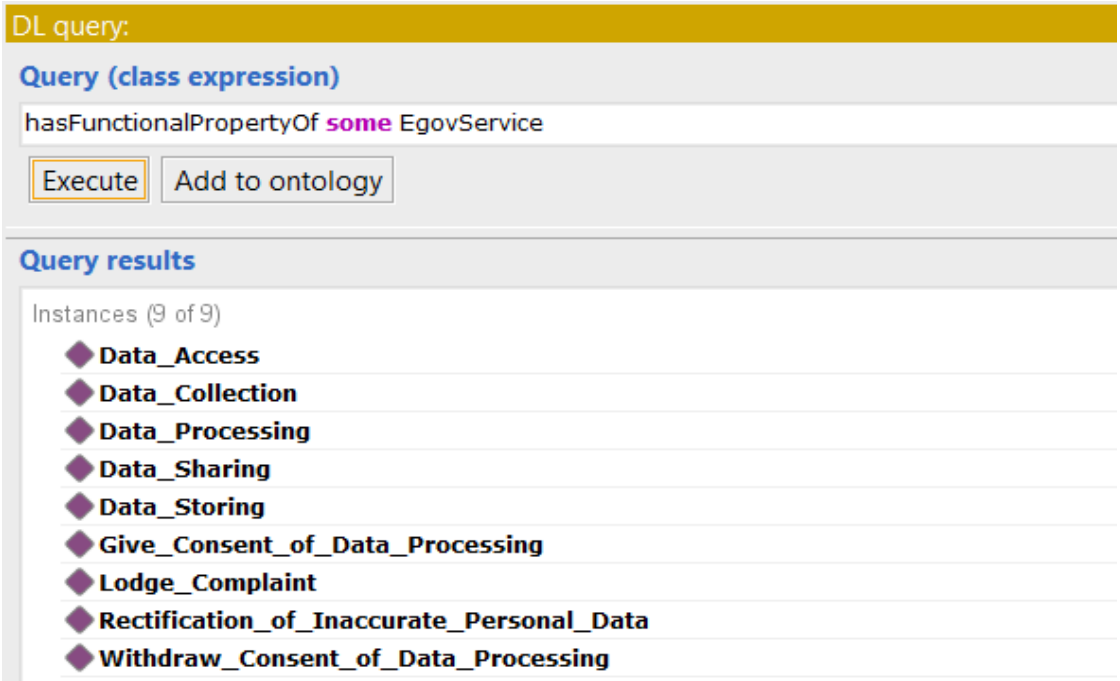


Figure 39: E-Service System Requirements from GDPR

Furthermore, Figure 40 presents the query results of the system non-functional requirements or quality requirements referenced in the GDPR regulation are the Data Availability, Data Accessibility, Data Confidentiality, Data Security, Data Accuracy, Data Timeliness, Data Portability, Data Resilience requirements that define the quality characteristic of the system in processing personal data.

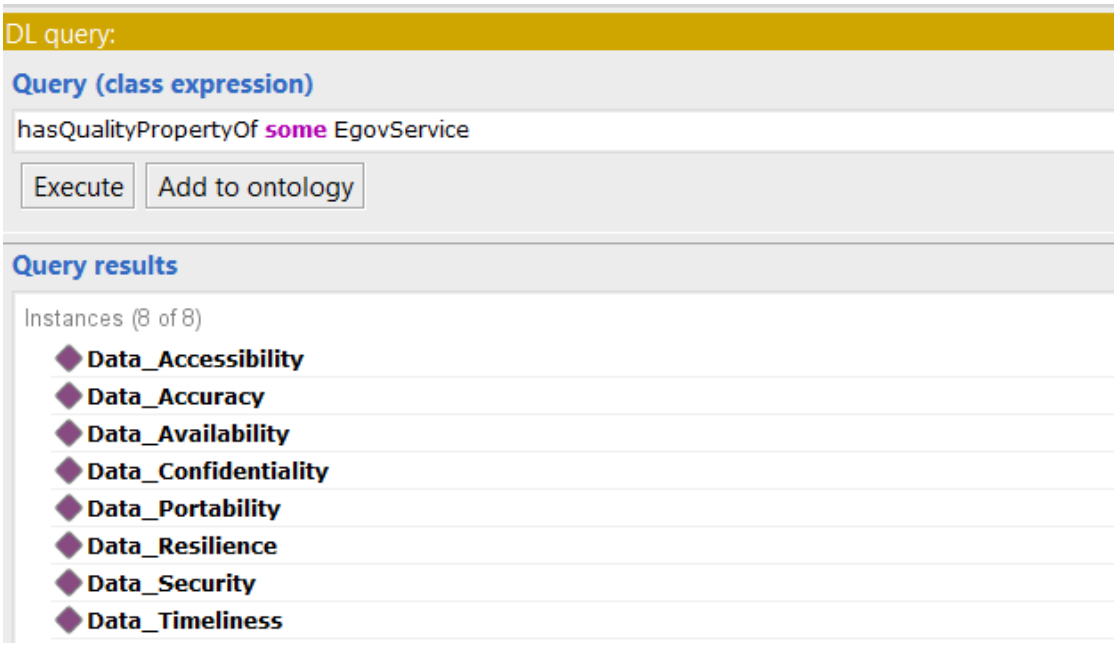


Figure 40: Quality Requirements of E-Services from GDPR

In Figure 41-44, the following queries (along with their results) are presented:

- What are the action enabler rules from the GDPR regulation that trigger some actions to be performed in the E-Government system development based on some defined conditions?
- What are the restrictions placed by the new GDPR regulation in the operations and development of the E-Government systems?
- What are the formulas in automated calculation to be used in E-Government system operation defined by the GDPR regulation?
- What are the GDPR rules that make an association between various entities in the E-Government system in formulating data models?

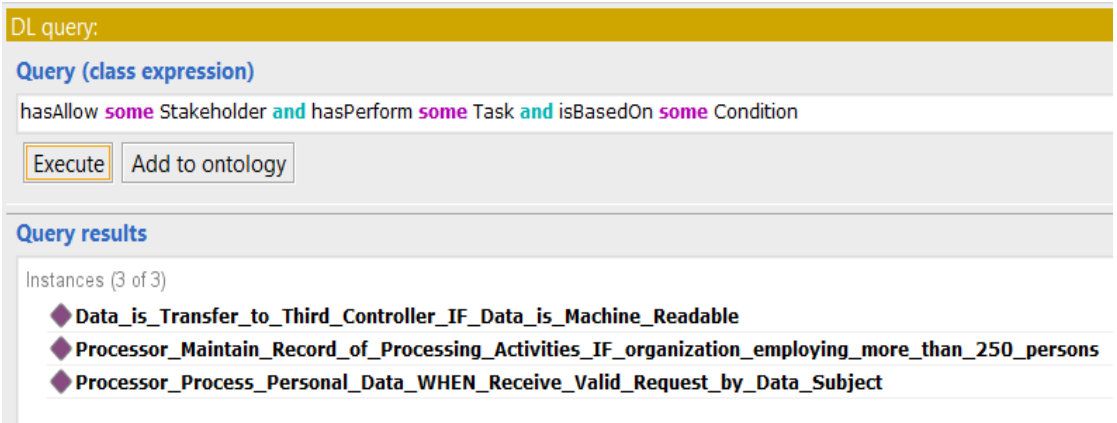


Figure 41: Action Rules in E-Government system from GDPR

Figure 41 presents the query results of the actions enabling rules referenced in the GDPR regulations in the E-Government system development. For example, the rules that define the data processors process personal data WHEN receive valid request by

data subject, allowing the processor to process personal data upon receiving a valid request by the data subject, The processor maintain record of processing activities IF organization employing more than 250 persons rule, and the data is transfer to third controller IF data is machine readable rule.

Figure 42 presents the query results of the restrictions rules referenced in the GDPR regulations in the E-Government system development. For example, the constraint rule that defines the controller shall provide personal data to data subject WITHIN one month of receipt the request. Also, the rule that defines the data controller shall report personal data breach BY 72 hours to the supervisory authority.

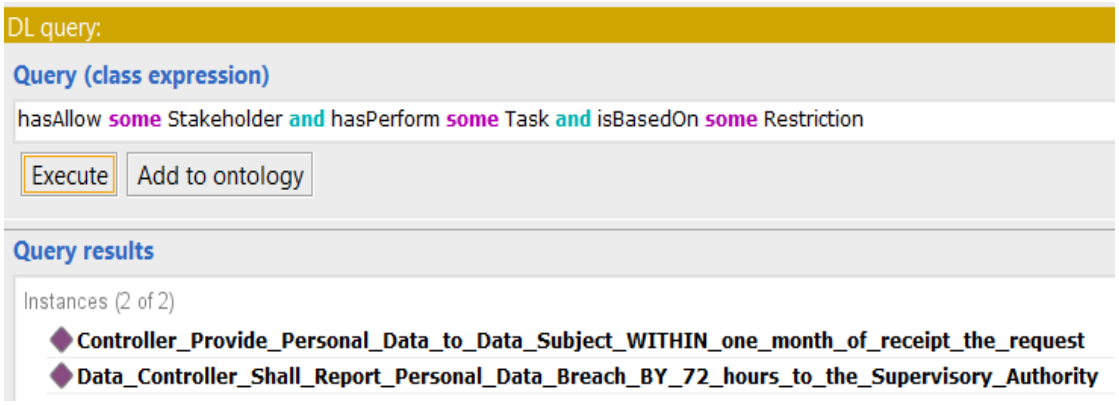


Figure 42: Restrictions placed by GDPR in the E-Government systems

Figure 43 presents the query results of the regulatory rules presents formulas in the system operation or calculation referenced in the GDPR regulations in the E-Government system development. For example, administrative fine computation rules for data controller liability in the case of data processing regulation violation, mapped to the EGRRC ontology as computation rules (e.g. calculation of the fine up to 2 percent of annual turnover or up to 10M€ whichever is higher).

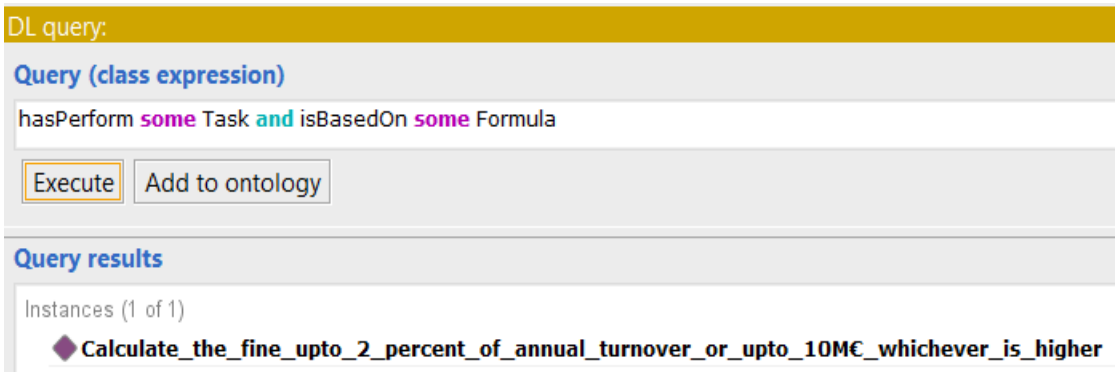


Figure 43: Computation rules in E-Government systems from GDPR

Furthermore, Figure 44 presents the query results of the facts rules that describe various relationship associations between the system entities referenced in the GDPR regulations in the E-Government system development. For example, an association

between the personal data and data subject needs to exist (e.g., every personal data has identification to the data Subject), as well as an association between the data subject and data controller (e.g., every data subject has a unique identification to the respective data controller).

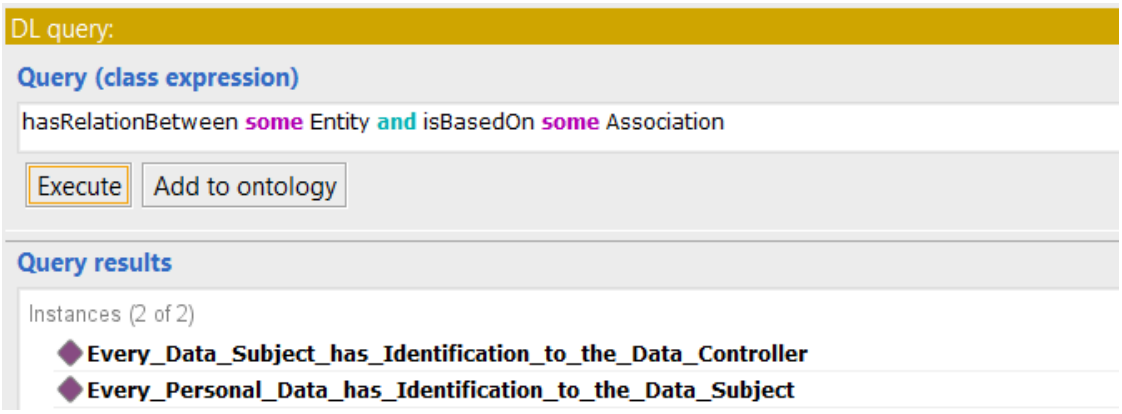


Figure 44: Associations made between entities in GDPR

In Figure 45-50, the following queries (along with their results) are presented:

- What is the priority level of the regulatory requirements that need to comply with every principle in the rule but does not impose a severe impact of noncompliance?
- What is the priority of the regulatory rule that has 10M€ EU fine for noncompliance and unauthorized access of encrypted data?
- What regulatory rules are obligatory and optional on the data controller in exercising the rights of the data subject?
- What regulatory rules are dynamic in nature and have some ambiguities in the system's operational process?

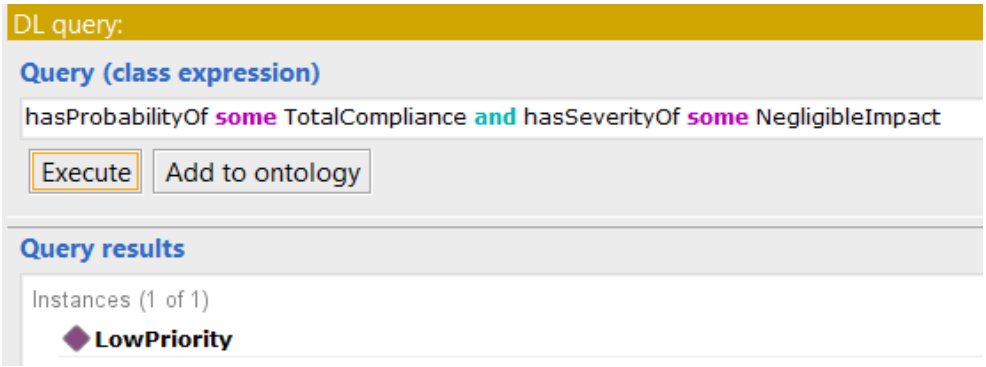


Figure 45: Priority of Compound Rules which has marginal impact

Figure 45 presents the query results of the priority level of the regulatory requirement which has compound rules and has a marginal impact on non-compliance. For example, in GDPR, the instruction transfers personal data to other controller based on data Subject consent AND if data process with automated means defines Total

Compliance of the regulatory rule where the two rules are combined with the AND operator (both rules must comply to transfer personal data to the third controller). And, the Partial Compliance combines rules using OR and EXCEPT operators. The instruction personal data processing requires data subject consent OR processing is necessary for legal obligation uses OR operator to combine two rules where any of these two rules must comply, and the instruction personal data processing concerning health and sexual orientation shall be prohibited EXCEPT explicit consent given by data subject, where the rule regarding the prohibition of processing personal data has an exception of that rule. The above regulatory rules are Compound Rule where multiple principles or clauses of an instruction are combined with AND OR operator. Furthermore, the instruction the controller shall maintain a record of the processing activities is a simple rule when it defines a single principle as in this case. GDPR also instructs the impact of noncompliance of the regulations into Significant Impact where administrative fine up to 10M€ for noncompliance of any regulation, and Negligible Impact where the unauthorized access of encrypted data may not cause any harm in the protected data processing.

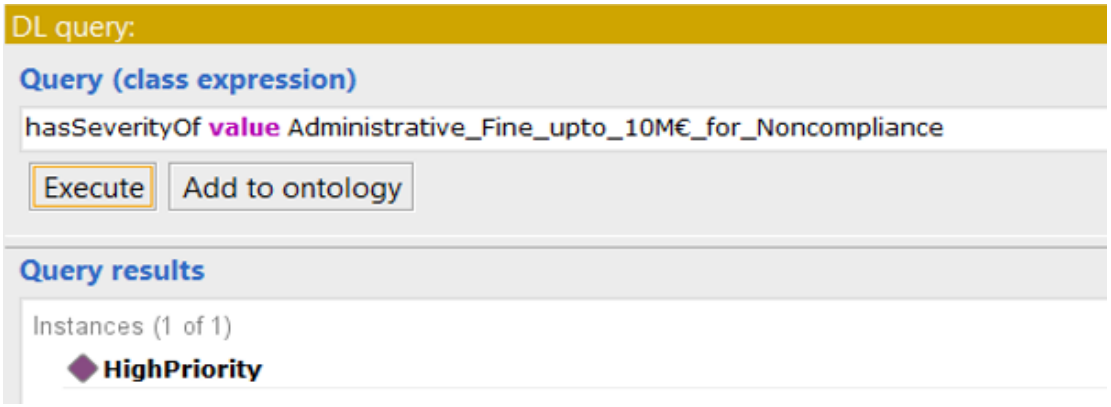


Figure 46: Priority of rules 10M€ EU fine for noncompliance

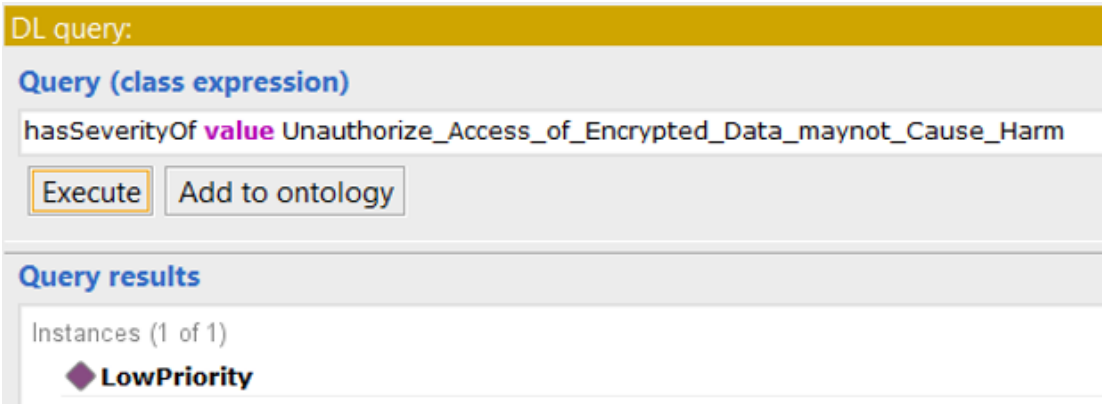


Figure 47: Priority of the rule has unauthorized access of encrypted data

Figure 46 presents the query results of the requirement's priority of regulatory rule that has 10M€ EU fine for noncompliance as High Priority regulatory rules. The

GDPR regulation instructs the significant impact of noncompliance with the obligatory regulatory rules where administrative fine up to 10M€ for noncompliance with any regulation.

Figure 47 presents the query results of the requirement's priority of regulatory rule that has unauthorized access to the encrypted data. The rule presents a negligible impact where the unauthorized access of encrypted data may not cause any harm in the protected data processing.

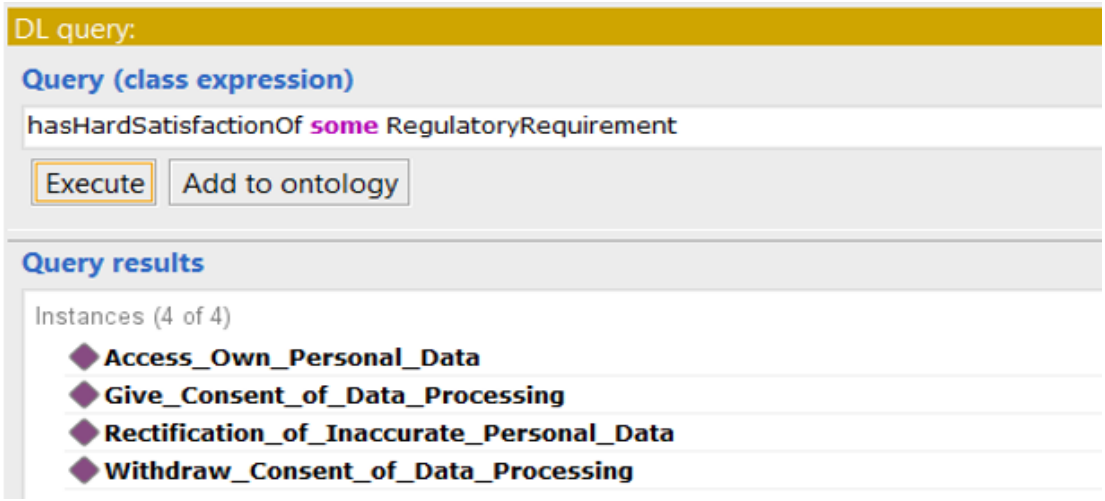


Figure 48: Obligatory regulatory rules in GDPR

Figure 48 presents query results of the regulatory requirements which are made obligatory by the GDPR regulation in the E-Government system development in processing personal data. The obligations of regulatory rules are the Data Subject's rights to give consent and withdraw consent of personal data processing, access own personal data, the rectification of inaccurate personal data which become an obligation to the data processor to comply.

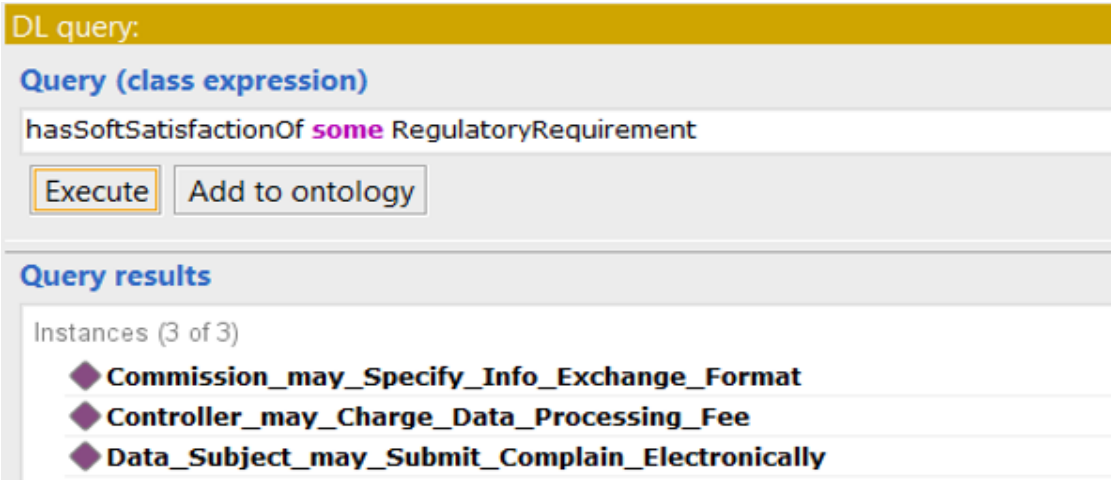


Figure 49: Privilege regulatory rules in GDPR

Figure 49 presents query results of the regulatory requirements which are treated as optional compliance in the E-Government system development. The privileges of the regulatory rules are the controller choice to charge reasonable data processing fee, commission's choice to specify information exchange format, data subject's choice to submit complain electronically which may be satisfied in the system but not required.

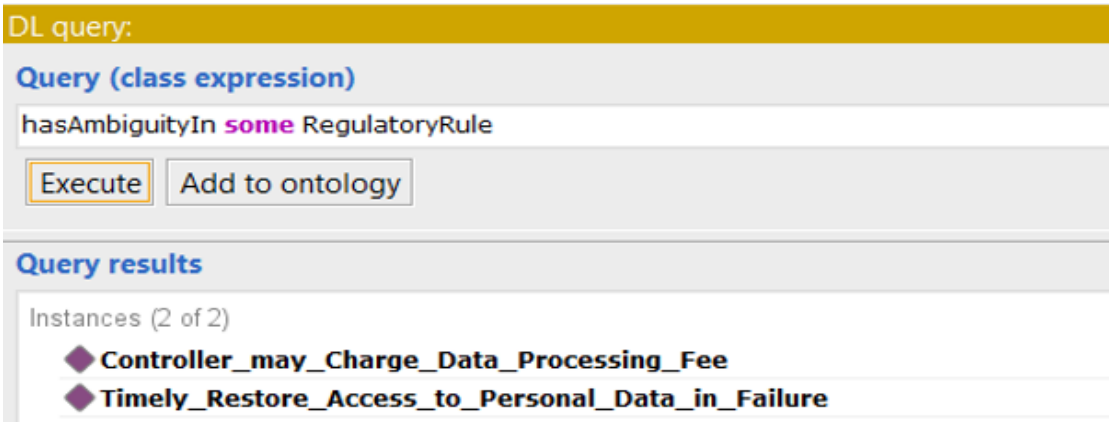


Figure 50: Dynamic regulatory rules in GDPR

Figure 50 presents query results of the regulatory requirements in GDPR regulation which has ambiguities in the description and dynamic in nature for scope of possible future amendments. For example, the dynamic rules are the reasonable data processing fee and restore availability and access to personal data timely in technical failure, since there are ambiguities with relation to deciding the amount of data processing fees and the time needs to restore the availability of personal data.

In Figure 51-52, the following queries (along with their results) are presented:

- Among the stakeholder of a system who are the receiver of system services based on the enacted GDPR regulation?
- Among the stakeholder who are the service provider based on the newly enacted GDPR regulation?

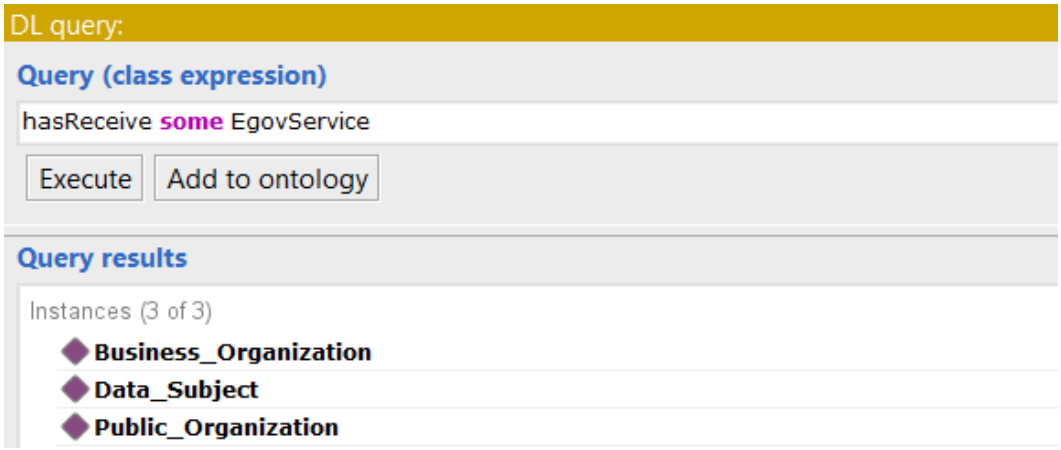


Figure 51: System users referenced in GDPR

Figure 51 presents the query results of system users based on the newly enacted GDPR regulation. For example, the Data Subjects or Citizens of an European country who request their own personal data, the Business Organizations who use the data for direct marketing, and the Public Organizations who use the personal data for investigating criminal acts or scientific research and statistical analysis are the system users according to the GDPR regulation.

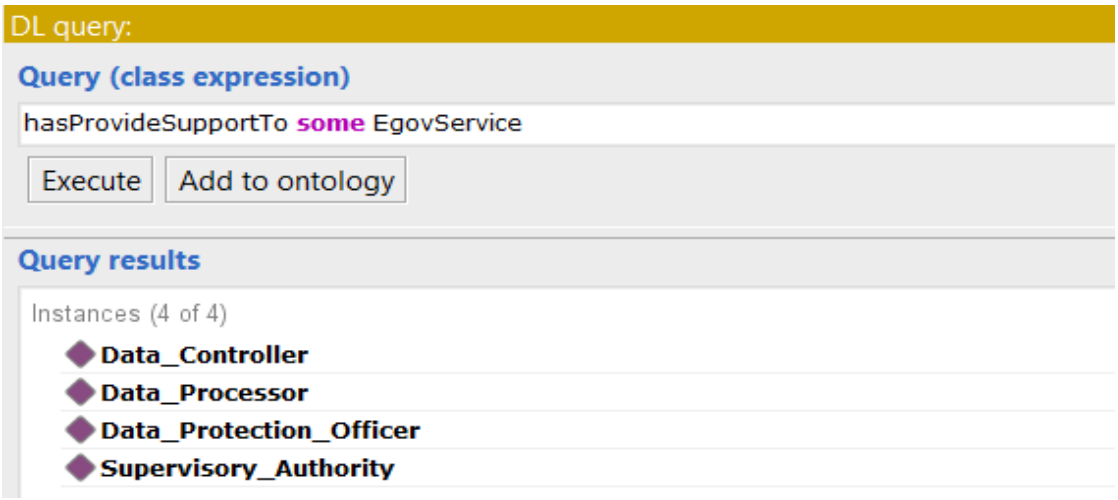


Figure 52: System service provider referenced in GDPR

Figure 52 presents the query results of system service provider based on the newly enacted GDPR regulation. For example, the Data Controller who determines the purposes and means of processing personal data based on the union or member state law, the Data Processor who processes the personal data on behalf of the controller, the Supervisory Authority who provides consultations to the controller and monitor the application of the regulations in each member states, the Data Protection Officer who has expertise knowledge in data protection law and advises the controller during the data protection impact assessment. Furthermore, the Donors of the system development are the European Union (EU) who funds the E-Government service development projects in the European zone, NGO is a non-profit charitable organization who also funds for improving the lives of the poor citizens in a country, and the funds also come from the National Government to digitize the government operations and provide electronic services to the citizens and business organization.

3.7 Remarks on EGRRC Ontology

For the conceptualization and implementation of the EGRRC ontology in the protege, a wide review of the existing literature has been performed. From the literature review of existing ontologies and general E-Government literature, initially 41 concepts have been extracted and presented in Table 2 and 3. The initially identified concepts from existing literature are then analyzed and extended to a total of 62 classes that describe the concepts of regulatory requirements compliance in the EGRRC ontology. The classes are then represented in a class hierarchy that has 13 parent classes that

describe the general concepts of the EGRRC ontology and usually answers the queries (e.g., requirements origin, regulation objective, E-Government services, etc.), and 49 subclasses derived from the parent classes that describe the specific properties and instances of the EGRRC ontology. There are 49 class properties that describe the relationships among the classes in EGRRC ontology. There are 75 actual relations have been made among the classes based on the class properties, and 10 relations have been inferred by the protégé reasoner in the EGRRC ontology.

The E-Government researcher and practitioner can use this framework as a knowledge repository to understand the interrelated concepts of regulatory requirements compliance in the E-Government system development. For the future studies, it would be interesting to couple the EGRRC ontology with technological concepts (or according to the external ontologies describing them), so that the guidance to the stakeholders also include guidelines around technical modifications that need to be performed for the IT systems to adapt to newly introduced legislative actions that affect them. This need has been addressed in the Chapter 4 by introducing the CISMET ontology which describes the system developer's guidelines around the technical modification of the E-Government information system development.

Chapter 4: CISMET Ontology Framework

The results of the systematic literature review (SLR) are presented here in Table 5. The elements of the regulatory Compliant Information System developMEnT (CISMET) ontology are extracted by reviewing the existing ontologies presented in the information system development domain. Specifically, for the reuse of the existing ontologies, this is based on the spirit of the Linked Data paradigm (Bizer, 2009), an approach to cross-reference elements from existing ontological vocabularies in order to enhance reusability and extension of concepts.

4.1 Existing Ontologies in System Development Domain

The following table illustrates the ontology elements of regulatory requirements compliant information system development. In each table entry, the 'Ontology' field provides the name and references of the existing ontologies in the information system domain and the 'Main Focus' field presents the primary contributions of the ontologies. The 'Class Hierarchy' field presents the hierarchy of classes extracted from existing ontology descriptions, the 'Class Property' field presents the interrelations between the classes, the 'Triple' field presents the relationships among the subject class and object class through class properties. It also presents the origins of the classes and properties (from which ontology are imported/extracted). The subject class, object class, and the class properties (i.e., predicates) in the triple are leveled with alphabetical order. For example, the subject class level with 'a' has a relationship with object class level with 'a' through the class property level with 'a'.

Table 5: CISMET ontology elements from existing ontologies

ONTOLOGY Name	**ISD ontology (Leppanen, 2006); TestTDO ontology (Tebes et al., 2020)**
Ontology Main Focus	The ontology is composed of concepts, relationships and constraints referring to the purposes, actors, actions, and objects of information system development.
Derived Class Hierarchy and Class Properties	**Classes Hierarchy:** • *Superclass:* SystemGoal [Subclass: HardGoal, SoftGoal] **Class Properties**: • isRegulatoryGoalOf class property describes the relationships between the RegulatoryObjective class of EGRRC ontology with the SystemGoal class of ISD ontology where the rule statements prescribe the outcome or goal of the information system project development. • hasContribute class property describes the relationships between the Operational Requirement class of EGRRC ontology with the

	HardGoal class of ISD ontology as the operational or functional requirements has predefined assessment criteria in the regulation to assess the fulfilment of the system development goal. • hasContribute class property also describes the relationships between the QualityRequirement class of EGRRC ontology with the SoftGoal class of ISD ontology as the non-functional quality requirements have general range of assessment criteria for assessing the system development goal. **Ontology Triple:** *Subject Class:* RegulatoryObjective (a), OperationalRequirement (b), Quality Requirement (c) (origin: EGRRC ontology) *Class Property:* isRegulatoryGoalOf (a) (origin: CISMET ontology), hasContribute (b, c) (origin: I* ontology) *Object Class:* SystemGoal (a), HardGoal (b), SoftGoal (c) (origin: ISD ontology)
ONTOLOGY Name	**Project System (ProSys) ontology (Stumpe, 2018)**
Ontology Main Focus	The ontology discusses the influences of project objectives and goals in the project development environment for their application in complex situations.
Derived Class Hierarchy and Class Properties	**Classes Hierarchy:** • *Superclass:* SystemGoal [Subclass: SoftGoal] **Classes Properties:** • hasCreate class property describes relationships between the Regulatory Requirement class of EGRRC ontology with the SystemGoal class of the ProSys ontology as the regulatory requirements define the needs or necessities in the system development which become the goal of the system development while agreed upon by the project stakeholder. **Ontology Triple:** *Subject Class:* RegulatoryRequirement (origin: EGRRC ontology) *Class Property:* hasCreate (origin: CISMET ontology) *Object Class:* SystemGoal (origin: Project System ontology)
ONTOLOGY Name	**Strategic Rational i* ontology (Beydoun, et al., 2014)**
Ontology Main Focus	The ontology describes the relationships between various goals, tasks, and actors in the system development.
Derived Class Hierarchy and Class	**Classes Hierarchy:** • *Superclass:* SystemGoal [Subclass: SoftGoal, HardGoal] **Classes Properties:** • hasPursue describes the relationship between eGovDonor class

Properties	of EGRRC ontology with the SystemGoal class of i* ontology as the funding organization is setting and pursuing the goal (hard or soft) of the information system development projects. **Ontology Triple:** *Subject Class:* eGovDonor (origin: EGRRC ontology) *Class Property:* hasPursue (origin: i* ontology) *Object Class:* SystemGoal (origin: i* ontology)
ONTOLOGY Name	**Software Process Ontology – SPO (Oveh & Egbokhare 2020); ODYSSEY Ontology (Olszewska & Allison, 2018); SEO Ontology (Wongthongtham et al., 2008); CMS Ontology (Niculescu & Rrausan-Matu, 2009); System Information Model - SIM Ontology (Van Ruijven, 2013)**
Ontology Main Focus	The ontology describes the Software Development Lifecycle (SDLC) phases which allow the software developer to select and use software development activities, tasks, and models.
Derived Class Hierarchy and Class Properties	**Classes Hierarchy:** • *Superclass:* SystemProcess [Subclass: RequirementAnalysis, SystemDesign, SystemDevelopment, SystemTesting, SystemMaintenance] **Classes Properties:** • providesRequirements class property describes the relationship between RegulatoryRequirement class of EGRRC ontology with the RequirementAnalysis class of the ODYSSEY ontology as it provides the regulatory requirements that need to be complient in the system development while collecting the requirements. • providesRequirements class property also describes the relationship between StandardDocument class of the EGRRC ontology with the SystemDesign class of SPO ontology as it provides various best practices and internatinal standard of the software and web interface design issues such as the ratio of cohesion and coupling in modulazing the software components, the web2.0 technology of the system/software interface design principles, etc. **Ontology Triple:** *Subject Class:* RegulatoryRequirement (a), StandardDocument (b) (origin: EGRRC ontology) *Class Property:* providesRequirements (a, b) (origin: CISMET ontology) *Object Class:* RequirementAnalysis (a) (origin: ODYSSEY SEO, CMS, SIM ontology), SystemDesign (b) (origin: SPO ontology)
ONTOLOGY Name	**ODE ontology (Falbo et al., 2003); CDO ontology (Henderson-Sellers**

	et al., 2014); DKDOonto ontology (Rocha, 2018)
Ontology Main Focus	The ontologies discuss the resources required in the software development activities in the software lifecycle process.
Derived Class Hierarchy and Class Properties	**Classes Hierarchy:** • *Superclass:* SystemResource [Subclass: SystemSoftware, SystemHardware, SystemData, HumanResource, BudgetResource, TimeResource] **Classes Properties:** • hasDetermine class property describes the relationship between RuleComponent class of the EGRRC ontology with the System Software and SystemHardware class of ODE ontology as it defines the hardware device and software application resources to be used in the information system development. • providesRestriction describes the relationship between the ConstraintRule class of EGRRC ontology with the SystemData TimeResource and BudgetResource as the constraint rules restict access of protected private data as well as time and budget of the project. **Ontology Triple:** *Subject Class:* RuleComponenet (a), ConstraintRule (b) (origin: EGRRC ontology) *Class Property:* hasDetermine (a), providesRestriction (b) (origin: CISMET ontology) *Object Class:* SystemSoftware(a), SystemHardware(a), SystemData(b) (origin: CISMET ontology), TimeResource (b), BudgetResource (b) (origin: ODE, CDO, DKDOonto ontology)
ONTOLOGY Name	**COPri ontology (Gharib et al., 2020); System Maintenance (SysMTN) ontology (Kitchenham et al., 1999)**
Ontology Main Focus	The ontologies describe various private confidential and public open access data. Also discuss corrective and adaptive maintenance work in the system operation. Also, discusses the change control process of evaluating the changes requests to approve or disapprove the system modification request.
Derived Class Hierarchy and Class Properties	**Classes Hierarchy:** • Superclass: SystemMaintenance [Subclass: SystemCorrection, SystemEnhancement] • Superclass: SystemData [Subclass: PrivateData, PublicData] **Classes Properties:** • hasEnforce class property describes the relationships between the DynamicRule class of the EGRRC ontology with the System Maintenence class of the SysMain ontology as sometimes the

	maintenance activity is driven by the amendment or introduction of new rules in the regulations. • hasMaintenancePriority class property describes the relationship between the CompliancePriority class of EGRRC ontology with the SystemMaintenance class of SysMain ontology which will help the system analyst with the control of system change request with high and low priorities of the maintenance works. • needsData and providesPrivateData class properties describe the relation between the PrivateData class of COPri ontolgoy and SystemMaintenance class as it describes the type of data needed in maintenance tasks. **Ontology Triple:** *Subject Class:* DynamicRule (a), CompliancePriority (b) (origin: EGRRC ontology), SystemMaintenance (c) (origin: System Maintenance ontology), PrivateData (d) (origin: COPri ontology) *Class Property*: hasEnforce (a), hasMaintenancePriority (b), needsData (c), providesPrivateData (d) (origin: CISMET ontology) *Object Class:* SystemMaintenance (a, b, d) (origin: System Maintenance ontology), PrivateData (c) (COPri ontology)
ONTOLOGY Name	**Software Process Ontology – SPO (Oveh & Egbokhare, 2020); Software Maintenance Project Management (SMPM) ontology (Ruiz et al., 2004); CDO ontology (Henderson-Sellers et al., 2014)**
Ontology Main Focus	The ontology describes the dynamic issues related to the management of maintenance tasks in various projects of software system development.
Derived Class Hierarchy and Class Properties	**Classes Hierarchy:** • *Superclass:* SystemMaintenance [Subclass: SystemCorrection, SystemEnhancement] • *Superclass:* HumanResource [Subclass: ProjectTeam] **Classes Properties:** • needsEnhancement describes the relationship between Privilege class of EGRRC ontology with the SystemEnhancement class of SMPM ontology as most of the maintenance work comes along with the enhancement of the system capacity and use. • needsCorrection describes the relationship between Obligation class of EGRRC ontology with the SystemCorrection class of CISMET ontology as the problems or errors in the system description must be corrected in the system operation. • hasToBePerformedBy class property describes the relationship between DevelopmentRequirements class of EGRRC ontology with the ProjectTeam class of CISMET ontology as it defines the project activities that need to be performed by the project team in the system development project.

	Ontology Triple: *Subject Class:* Privilege (a), Obligation (b), DevelopmentRequirements (c) (origin: EGRRC ontology) *Class Property:* needsEnhancement (a), needsCorrection (b) (origin: CISMET ontology), hasPerformedBy (c) (origin: CDO ontology) *Object Class:* SystemEnhancement (a), SystemCorrection (b) (origin: Software Maintenance Project Management ontology, SPO ontology), ProjectTeam (c) (origin: CISMET ontology)
ONTOLOGY Name	**Rule based Framework (ROF) ontology (Yanuarifiani et al., 2020); Software Project Management ontology - SPM (Bastos et al., 2018); System Development (SysDev) Ontology (Hallberg et al., 2014);**
Ontology Main Focus	The ontologies discuss the fundamental definitions of general concepts, description concepts, realization concepts, and appearance concepts, also their dependencies and relationships in the systems development activities.
Derived Class Hierarchy and Class Properties	**Classes Hierarchy:** • *Superclass:* Activity [Subclass: SystemActivity, ProjectActivity] **Classes Properties:** • providesFunctionality describes the relation between Regulatory Rule class of EGRRC ontology and SystemActivity class of CISMET ontology as it defines the permissible tasks, restrictions, and performance constraints of the system and project activities enforced by the regulations. • providesFunctionality class property also describes the relation between DevelopmentRequirement class of EGRRC ontology and ProjectActivity class of CISMET ontology as it defines the project development constraints. • hasTrigger describes the relations between ActionRule class of EGRRC ontology and Activitiy class of CISMET ontology as it describes the triggering events of an action to be performed in the system and project operation. • hasExecute describes the relations between ServiceProvider class of EGRRC ontology and ProjectActivity class of CISMET ontology as it describes the responsible role to perform the project development activities. **Ontology Triple:** *Subject Class:* RegulatoryRule (a), DevelopmentRequirement (b), ActionRule (c), ServiceProvider (d) (origin: EGRRC ontology) *Class Property:* providesFunctionality (a, b), hasTrigger (origin: CISMET ontology), ProjectActivity (d) (origin: ROF ontology) *Object Class:* Activity (a, c), ProjectActivity (b, d) (origin: System Development ontology, Software Process, and CISMET ontology)

ONTOLOGY Name	**Project Management Process (PMP) Ontology (Hughes, 2010)**
Ontology Main Focus	The ontology describes the project management procedures prescribed by the Project IN Controlled Environment (PRINCE)
Derived Class Hierarchy and Class Properties	**Classes Hierarchy:** • *Superclass:* HumanResource [Subclass: SystemUser, SystemSupplier] **Classes Properties:** • hasAuthorize class property describes the relationship between eGovUser class of EGRRC ontology with the SystemUser class of PMP ontology as it provides the system user with legitimacy of using the system based on the regulations. • isResponsibleRoleOf describes the relationship between ServiceProvider class of EGRRC ontology and SystemSupplier class of PMP ontology as it defines what roles are responsible or obliged by the regulations for giving services to the system users. **Ontology Triple:** *Subject Class:* eGovUser (a), ServiceProvider (b) (origin: EGRRC ontology) *Class Property:* hasAuthorize (a), isResponsibleRoleOf (b) (origin: CISMET ontology) *Object Class:* SystemUser (a), SystemSupplier (b) (origin: Project Management Process ontology)
ONTOLOGY Name	**Project Management Knowledge (PMK) ontology (Sheeba, et al., 2012); DKDOonto ontology (Rocha, 2018); Requirement Traceability (ReQT) ontology (Wibowo & Davis, 2020);**
Ontology Main Focus	The ontologies describe the artifacts and human resources to be used in the activities regarding project management body of knowledge (PMBOK) aiming to support in the distributed system development activities.
Derived Class Hierarchy and Class Properties	**Classes Hierarchy:** • *Superclass:* HumanResource [Subclass: ProjectTeam, SystemUser] • *Superclass:* SystemArtifact [*Subclass:* SystemSpecification, DsignSpecification] **Classes Properties:** • providesRestriction class property describes the relationship between ConstraintRule class of EGRRC ontology with the HumanResource and SystemArtifact classes of PMK and DKDOonto ontology as the constraint rules restict some roles in perfroming some activities, also provide restriction on the entities

	of system requirements and design artifacts. **Ontology Triple:** *Subject Class:* ConstraintRule(a) (origin: EGRRC ontology) *Class Property:* providesRestriction(a) (origin: CISMET ontology) *Object Class:* HumanResource(a), SystemArtifact(a) (origin: PMK ontology, DKDOnto ontology)
ONTOLOGY Name	**E-Service (eSER) ontology (Annamalai et al., 2011; Bianchini et al., 2006)**
Ontology Main Focus	The ontology discusses the classification of electronic services according to branches and its processes.
Derived Class Hierarchy and Class Properties	**Classes Hierarchy:** • *Superclass:* SystemService [Subclass: DataService] **Classes Properties:** • hasInitiate describes the relationship between eGovService class of EGRRC ontology with the SystemService class of the E-Service ontology as many services initiation are originated by the regulations. • The class property needsData and providesPrivateData also describes the relation between the PrivateData class of CISMET ontology and SystemService class of E-Service ontology as it describes the type of data needed in the services. **Ontology Triple:** *Subject Class:* eGovService (a) (origin: EGRRC ontology), SystemService (b) (origin: E-Service ontology), PrivateData (c) (origin: CISMET ontology) *Class Property:* hasInitiate (a), needsData (b), providesPrivateData (c) (origin: CISMET ontology) *Object Class:* SystemService (a, c) (origin: e-Service ontology), PrivateData (b) (origin: CISMET ontology)
ONTOLOGY Name	**Service System (SerSys) ontology (Lemey & Poels, 2011); SoaML Service ontology (Yustianto et al., 2018)**
Ontology Main Focus	The ontology discusses mapping of fundamental service system concepts on the service theories and frameworks in service domain.
Derived Class Hierarchy and Class Properties	**Classes Hierarchy:** • *Superclass:* SystemService [Subclass: AuthenticationService] **Classes Properties:** • hasRightToReceive class property describes the relationship between the eGovUser class of the EGRRC ontology with the SystemService class of SerSys ontology as it defines the system user who has the right to get access of their expected services.

	• hasDutyToProvide describes the relationship between Service Provider class of EGRRC ontology with the SystemService class of SerSys ontology as it defines the enforced duty on the service provider to respond the user request for service. **Ontology Triple:** *Subject Class:* eGovUser (a), ServiceProvider (b) (origin: EGRRC ontology) *Class Property:* hasRightToReceive (a), hasDutyToProvide (b) (origin: CISMET ontology) *Object Class:* SystemService (a, b) (origin: SerSys, SoaML ontology)
ONTOLOGY Name	**Software Process Ontology – SPO (Oveh & Egbokhare, 2020); Rule-Based Ontology Framework (ROF); TestTDO ontology (Tebes et al., 2020)**
Ontology Main Focus	The ontology describes the Software Development process which allow the software developer to select and use various software development activities, tasks, and models in the software project development.
Derived Class Hierarchy and Class Properties	**Classes Hierarchy:** • *Superclass:* SystemProcess [Subclass: RequirementAnalysis, SystemDesign, SystemDevelopment, SystemTesting, SystemMaintenance] **Classes Properties:** • providesRestriction class property describes the relationship between ConstraintRule class of the EGRRC ontology with the SystemDevelopment class of SPO ontology as the constraint rules provides coding standards, incremental development, language specification, etc. while writing codes and developing the software products. • hasEnforce class property describes the relationship between Regulatory Requirement class of the EGRRC ontology with the SystemTesting class of SPO and TestTDO ontology as there might some regulatory requirements which are enforced by the regulations to monitor the system operations and project activities for quality control of the information system development. • hasGenerate class property describes the relationship between SystemProcess class of SPO and ROF ontologies and Activity class of CISMET, SysDev ontologies as various system process and phases are consisting of the system's operation and project development activities. **Ontology Triple:** *Subject Class:* ConstraintRule (a), RegulatoryRequirement (b) (origin: EGRRC ontology), System Process (origin: SPO ontology, ROF ontology)

	Class Property: providesRestriction (a), hasEnforce (b), hasGenerate (c) (origin: CISMET ontology) *Object Class:* SystemDevelopment (a), SystemTesting (b), Activity (c) (origin: SPO ontology, TestTDO ontology, SysDev ontology, CISMET)
ONTOLOGY Name	**CloudFNF Ontology (Al-Sayed et al., 2020); TestTDO ontology (Tebes et al., 2020); Requirement Traceability (ReQT) ontology (Wibowo & Davis, 2020);**
Ontology Main Focus	The ontologies discuss various artifacts such as system specification, design specification, test case and testing specifications as a result of various system development process and activities.
Derived Class Hierarchy and Class Properties	**Classes Hierarchy:** • *Superclass:* SystemArtifact [Subclass: SystemSpecification, DesignSpecification, TestingSpecification] • *Superclass:* SystemSpecification [Subclass: TechnicalProperty, ManagementProperty] **Classes Properties:** • providesRequirements class property describes the relationship between RegulatoryRequirement class of the EGRRC ontology with the SystemArtifact class of ReQT, CloudFNF, and TestTDO ontologies (e.g., System Specification, Design Specification, Testing Specification) as it provides requirements for various system, design, testing artifacts. • In particular providesRequirements class property describes relationship between the SystemRequirement class of the EGRRC ontology with the TechnicalProperty class of CloudFNF ontology. It also describes the relations between DevelopmentRequirement class of EGRRC ontology with the ManagementProperty class of CoudFNF ontology as it provides various properties regarding project development. • providesRestriction class property describes the relationship between ConstraintRule class of EGRRC ontology with the SystemArtifact class of CISMET ontology as the constraint rules provides various restrictions on various types of System Artifacts. **Ontology Triple:** *Subject Class:* RegulatoryRequirement (a), SystemRequirement (b), DevelopmentRequirement (c), ConstraintRule (d) (origin: EGRRC) *Class Property:* providesRequirements (a, b, c), providesRestriction (d) (origin: CISMET ontology) *Object Class:* SystemSpecification (a), DesignSpecification (a), Testing Specification (a) (origin: ReQT ontology, TestTDO ontology), TechnicalProperty (b) (Origin: CloudFNF), ManagementProperty (c) (origin CISMET ontology), SystemArtifact (d) (origin: CISMET)

Furthermore, Table 6 presents the summary of the triple descriptions in reutilizing, extending, and combining the existing vocabularies from the available ontologies to enhance their reusability and extension through the CISMET ontology. This is particularly useful in adapting to the concept of Linked Data paradigm while avoiding duplication of information (Bizer, 2009). In that context, CISMET defines a few subjects and objects where needed but mainly deals with defining new relationships (44 in total) through the use of 21 introduced predicates, acting as a link between the various concepts.

Table 6: Summary of the CISMET Triple description

Triple Descriptions	**Total Number**
Number of ontologies used in the CISMET ontology to import/extract ontology concepts	27
Number of subject classes from imported ontologies	22
Number of subject classes newly defined in CISMET ontology	2
Number of object classes from imported ontologies	27
Number of object classes newly defined in CISMET ontology	5
Number of predicates (i.e., class properties) from imported ontologies	4
Number of predicates introduced in CISMET ontology to define relationships	21
Number of relations made in the CISMET (i.e., relations between subject-object class)	44

4.2 CISMET Ontology Class Hierarchy

In OWL ontology, the classes are the main building blocks which present sets of individuals. The subclasses of specific concepts are described under the superclass of general concepts in the class hierarchy. The Things class is the parent of all classes in the ontology which by default puts all the classes as the subclass of Thing class. In protégé, there is no specific naming convention of class name, however, it is recommended to name the class with CamelBack notation which has capitalized words without any space in between (Horridge et al., 2004).

In Figure 53, The SystemGoal class defines the objective or motivation/intention of the system development. The SystemGoal can be classified further into HardGoal that represents the system goals which has predefined concrete assessment criteria to assess the fulfilment of system functionalities whereas the SoftGoal represents the system goals which has general ranges on a scale of assessment criteria to assess the fulfilment of nonfunctional quality attributes of the system. The SystemProcess class describes various systematic process or phases in the information system

development which can be primarily classified into five phases. In Requirement Analysis, all the relevant information and requirements of the system development projects are collected and recorded in the requirements specification document (SRS). In SystemDesign, the requirements from the analysis phase are designed into a system architecture. In SystemDevelopment, the system is being developed based on the system architecture. In SystemTesting, the developed system is being tested for any defects and user acceptance. And, SystemMaintenance describes the evolution of the system and various types of maintenance works in information system operations. The maintenance can be SystemCorrection which modifies the system in order to fix problems in the system whereas the SystemEnhancement modifies the system in order to improve the system functionality or prevent any potential errors that may occur in the future.

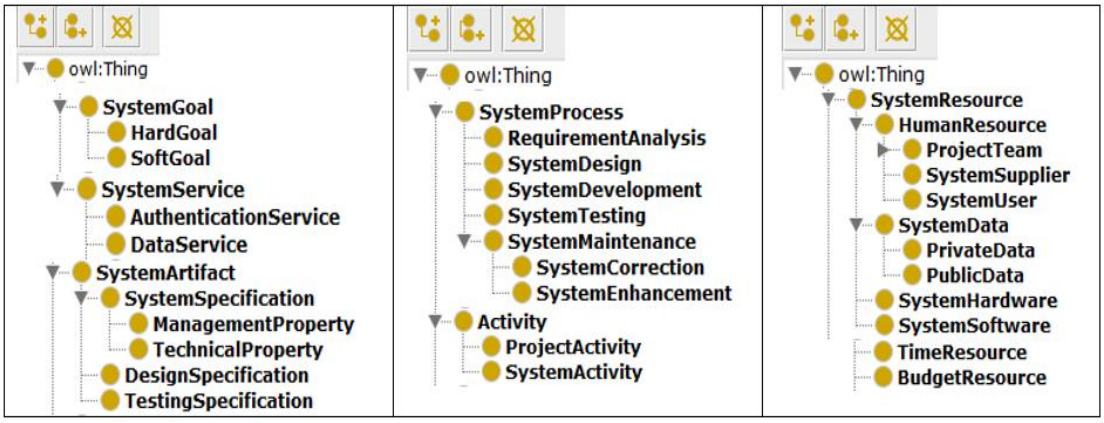


Figure 53: Class Hierarchy of CISMET Ontology

The SystemService class describes the e-services provided by the information system which can be classified into DataService mainly focus on the data as a service that provides various data services such as store and transfer data over cloud infrastructure. AuthenticationService facilitates the identity verification of providing services to the users and others. Activity class describes the set of tasks or permissible actions that is required to perform in the system development projects. The Activity is primarily divided into two type of activities. SystemActivity describes the task that needs to be performed by the system functionalities and ProjectActivity describes the task that needs to be performed in the project management activities.

SystemResource class describes the required type of resources to carry out the system/project activities. The resource can be SystemHardware is the device used in the system development, SystemSoftware is the software applications or tools used in system development. And, SystemData describes the information resource with the type of data used in processing the services requested by the system users. The system data can be PrivateData those are sensitive and protected to be used publicly and PublicData those can be shared publicly. And, HumanResource is the system roles which are group of authorities and responsibilities in the system development

specified in taking respective actions. The roles in system development project can be primarily classified into three categories. The SystemUsers are the main user of the system who uses the system for their needs. The SystemSuppliers are the responsible role to provide expected services to the users. And, the members of the ProjectTeam are the responsible role of the project development activities such as system analyst, designer, developer, etc. TimeResource and BudgetResource are the time and money required to be used in the project development to complete the system/project activities. The SystemArtifact class describes the work products produced by the system development process, for example, SystemSpecification is the requirements specification documents produced by the requirement analysis process. The system specification can have ManagementProperty that describes the project management constraints and plan in developing the system/software project, and TechnicalProperty that describes the technical concepts of the system/software which needs to be developed and deliver to the users such as system's functionality and non-functional quality properties. The DesignSpecification discusses the system design produced by the system design process such as UML use cases and class diagrams. The TestingSpecification documents discusses the test cases and test plan of monitoring and verifying the system operations and system development activities in the project development process.

4.3 Class Properties to Describe CISMET Ontology

The class properties describe the relationships among the classes of EGRRC ontology with CISMET ontology classes. In protégé, there is no specific naming convention of class properties, however, it is recommended to name the class properties in camelCase (i.e., lower case at the beginning and capitalized form of remaining words with no space in between).

In Figure 54, the goal of information system development is described by the class property isRegulatoryGoalOf from the regulations that identifies the system development goals based on the objectives of the regulations in EGRRC ontology. Also, the regulatory requirements from EGRRC ontology hasCreate the system development goals while these requirements are agreed upon by the project stakeholder to be implemented in the system development. The hard goals can be extracted from the operational requirements and soft goal of the system development can be extracted from quality requirements of the EGRRC ontology by using the hasContribute class property. Furthermore, the EGRRC ontology also declares the stakeholder who sets and pursues the fulfilment of the information system development goals from the funding organizations and user groups from the EGRRC ontology by the hasPursue class property.

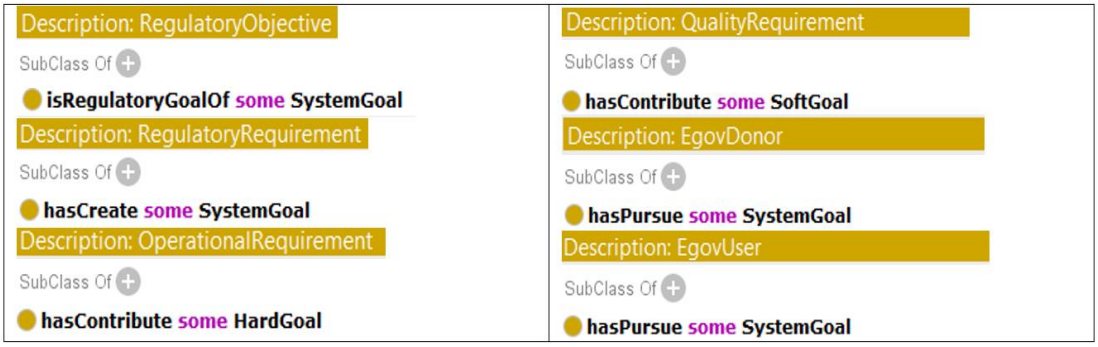


Figure 54: Class properties to describe system goal based on regulations

Figure 55 describes the services provided by the information system where these services are often initiated from the e-Gov Service class of EGRRC ontology by the hasInitiate class property which defines various type of services to be provided by the system based on the regulations. The providesRestriction class property restrict the access and share of protected personal data in producing the system services. The hasRightToReceive class property identifies the rightful users of the system services from the e-Gov User class of EGRRC ontology. And the class property hasDutyToProvide identifies the responsible person to respond the user's service request from the service provider class of EGRRC ontology based on the regulations. Furthermore, the system services those are using sensitive personal data can also be identified based on the needsData class property. And which private data are requested in the services processing can also be identified by the provides PrivateData class property from private data class. Furthermore, the class property ProvidesRequirements describes the required regulatory requirements for data and authentication services provided by the system operations from the system requirement class of EGRRC ontology.

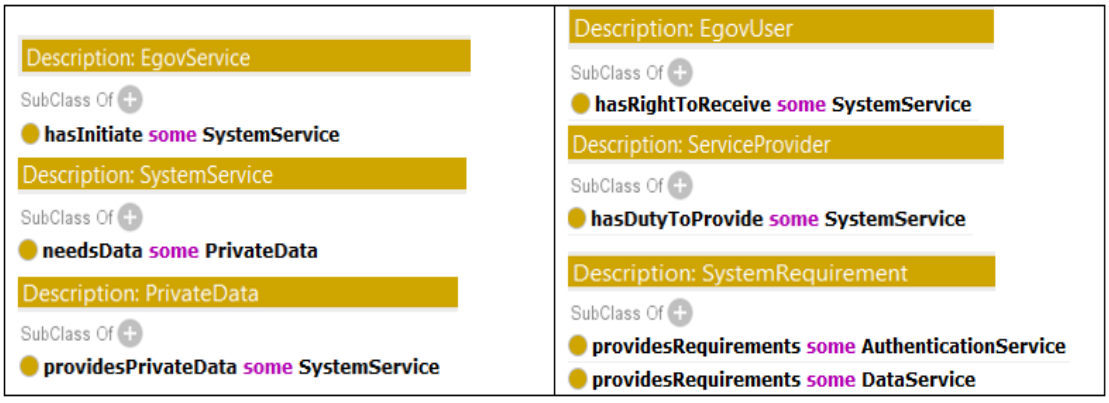


Figure 55: Class properties to describe system service based on regulations

Figure 56 describes the process of system development project. It provides the requirements from the regulations by the regulatory requirement class of the EGRRC ontology using the providesRequirements class property that needs to be compliant in the project. The maintenance task is often imposed in the system maintenance

process from the dynamic rule class of the EGRRC ontology by hasEnforce class property based on the regulation amendments. At the same time, the priority of system maintenance tasks to be compliant with the regulations can also be decided from the compliance priority class of the EGRRC ontology by hasMaintenance Priority class property. The maintenance tasks will be given high priority compliance when the regulatory rule needs to be totally compliant without any exception and has significant severity of failing to comply. On the other hand, the maintenance tasks will be given low priority compliance when the regulatory rule has partial compliance (i.e., has an exception to escape from obligation) and/or does not pose any significant concern for noncompliance.

Moreover, the system maintenance tasks which requires private data from the system data resource can be identified by the needsDataFrom class property, as well as which private data are requested to be used in system maintenance can also be extracted by the providesPrivateData class property from the PrivateData class. Furthermore, the system enhancement of the maintenance tasks can be found from the privilege class of the EGRRC ontology by needsEnhancement class property which describes the opportunistic maintenance for improving the system performance. And the correction tasks are made compulsory on the system maintenance work from the obligation class of EGRRC ontology by needsCorrection class property which describes the system maintenance tasks that are bound to perform by the regulation.

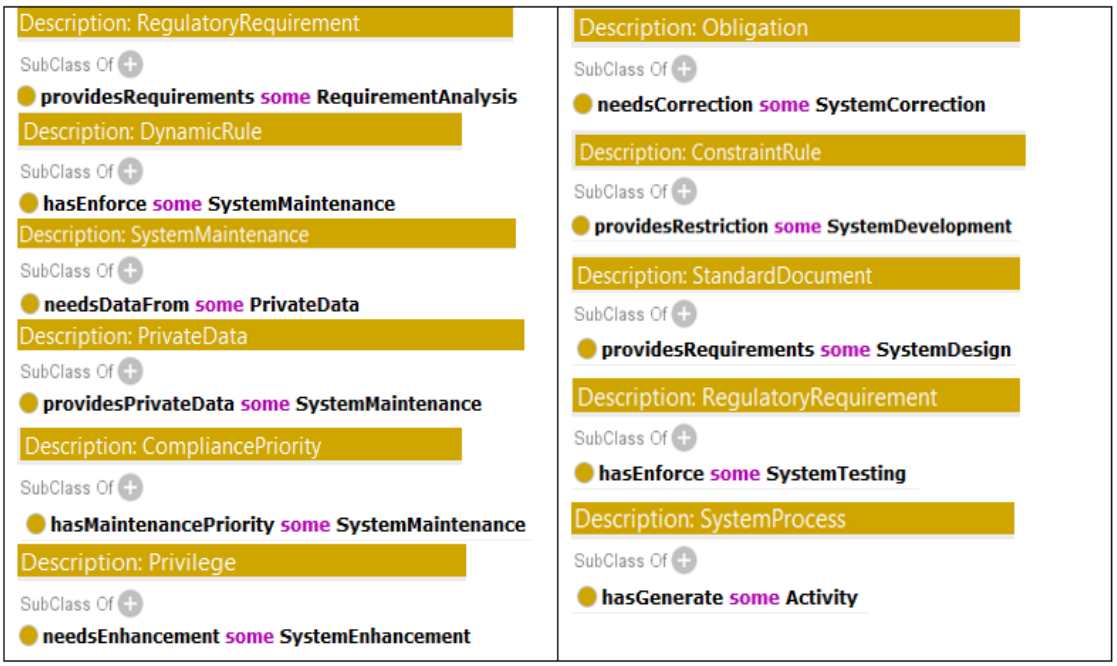


Figure 56: Class properties to describe system process based on regulations

The providesRestrictions class property provides some restrictions of the system development activities such as coding and implementation choice from the constraint rule class of the EGRRC ontology. The providesRequirements class property also provides the regulatory requirements for system design issues from standard

document class of external regulations such as modularity of software components and Web2.0 technology that provides the guidelines of web interface design according to the international standard. Furthermore, the hasEnforce class property describes the requirements regarding the system testing activities in the project development process from regulatory requirements class of the EGRRC ontology to monitor the development process and control the system quality. Finally, the hasGenerate class property provides various system and project management activities necessary to be performed by various system development process.

Figure 57 describes the activities based on regulations. The activities can be derived from the regulatory rules class of the EGRRC ontology by the providesFunctionality class property. Furthermore, the hasTrigger class property describes the triggering events of those system development activities from the action rules class of EGRRC ontology. The providesFunctionality class property also describes the project development activities from the development requirements class of EGRRC ontology. Furthermore, the class property hasPerformedBy describes the project activities performed by the project team from the development requirements class of EGRRC ontology. And providesRestriction class property describes the restrictions imposed by regulations upon the activities (i.e., system activity, project activity) from constraint rule class of the EGRRC ontology. Furthermore, the hasExecute class property describes the project activities need to be performed in the project development process from the service provider class of EGRRC ontology.

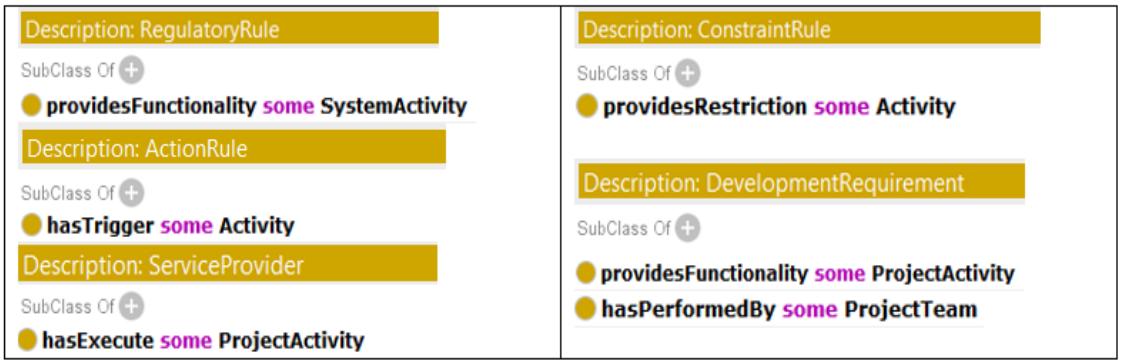


Figure 57: Class properties to describe activities based on regulation

Figure 58 describes the system resources based on regulations. The class property isResponsibleRoleOf describes the responsible roles of providing services to the users based on the regulations from the service provider class of EGRRC ontology. The hasAuthorize class property identifies the authorized users of the system from the e-Gov user class of the EGRRC ontology based on the regulations. Furthermore, the providesRestriction class property describes the restrictions imposed by regulations upon the human resources (i.e., project team, system user, and system supplier) private data, time and budget resources, and system artifacts from constraint rule class of the EGRRC ontology. The hasDetermine class property identifies the

resources regarding software application and hardware devices from the rule component class of the EGRRC ontology.

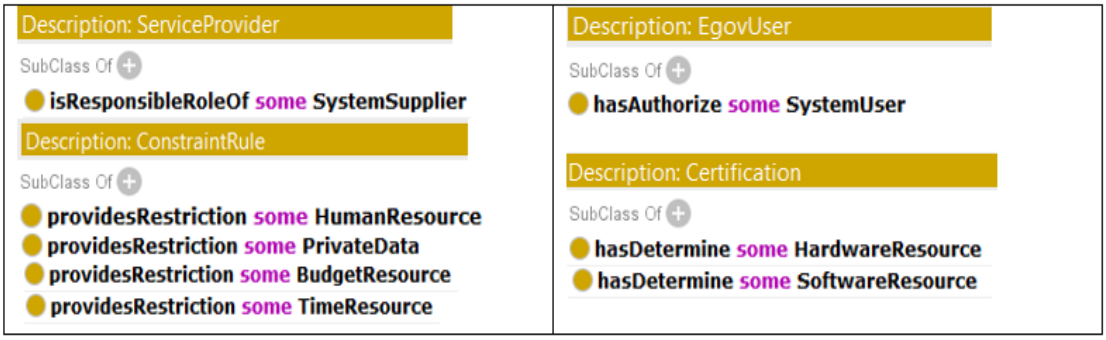


Figure 58: Class properties to describe system resources based on regulation

Figure 59 describes the system artifacts based on the regulations. The provide Requirements class property describes the various types of artifacts in the system or software development from the regulatory requirements class of EGRRC ontology. For example, the system specification describes the system/software requirements to be implemented in the system/software development, the design specification describes various diagrams such as use-case diagram, class diagram, activity diagram, context diagram, entity-relationship diagram to be used in the system development. And the testing specification defines various test cases and testing plan to be followed in the system/software development in order to monitor and verify the system/project properties. Furthermore, the system requirement class of EGRRC ontology describes the technical properties of the system specification and development requirements class of the EGRRC ontology describes the project management properties of the system/software project management specification. Moreover, the provides Restriction class property also describes the restrictions imposed by regulations upon various system artifacts from the constraint rule class of EGRRC ontology.

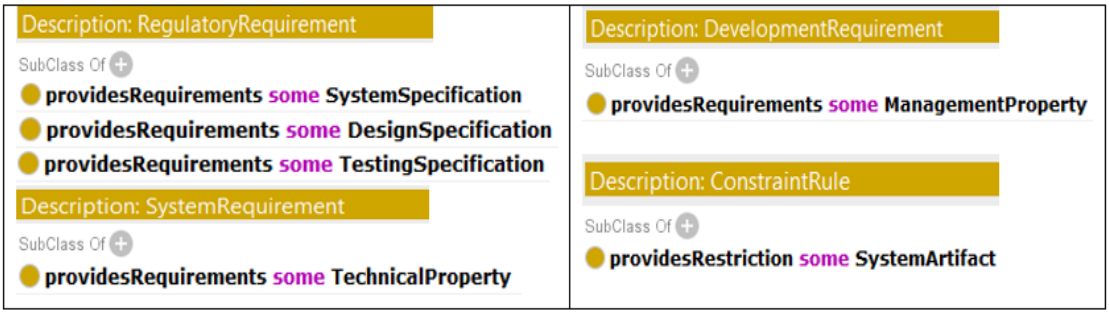


Figure 59: Class properties to describe system artifacts based on regulation

Figure 60 presents the interconnected concepts of regulatory requirements compliant information system development showing the interrelationships between the classes in the class hierarchy of different ontologies through various class properties.

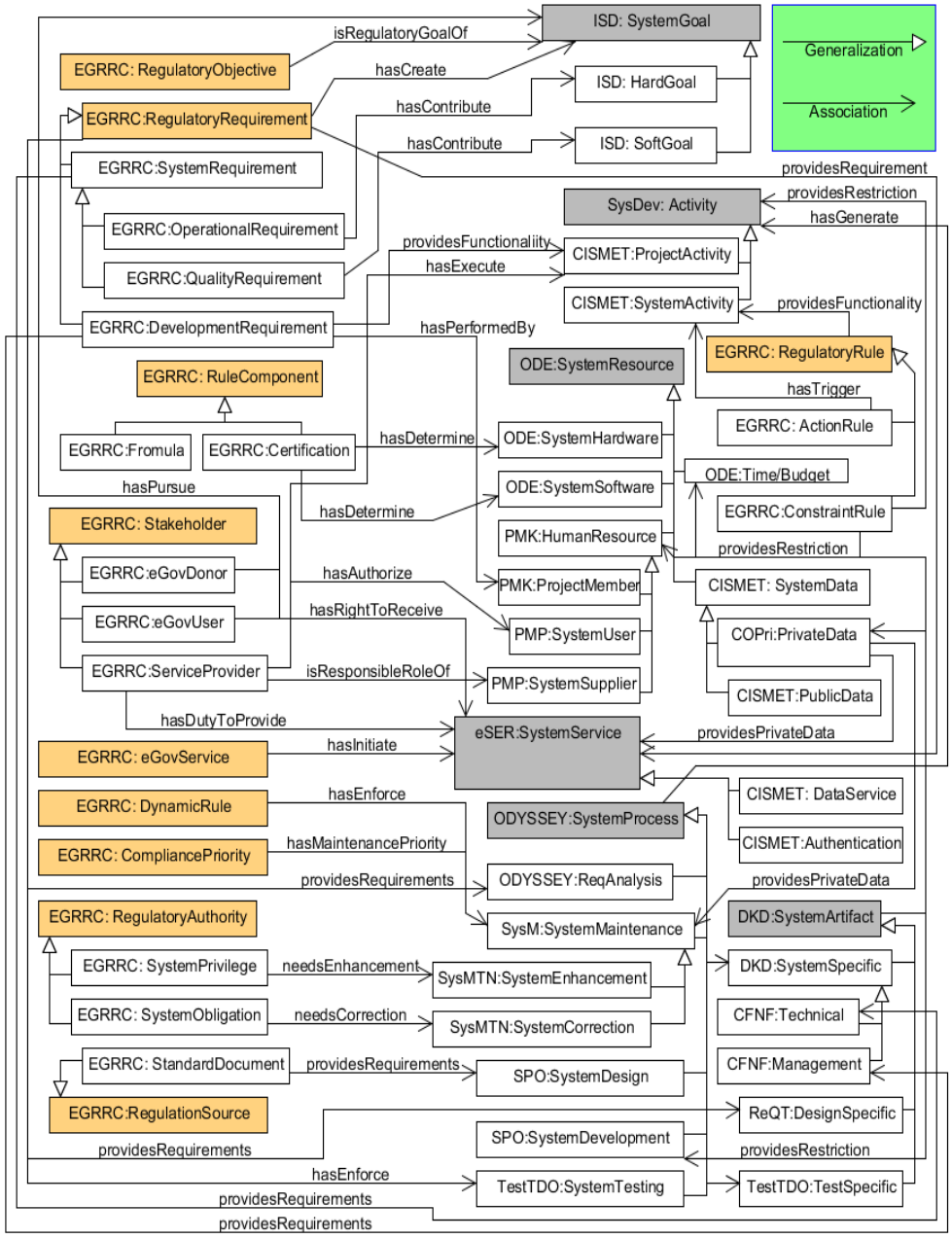


Figure 60: Compliant Information System Development Ontology (CISMET)

4.4 Quality Evaluation of the CISMET Ontology

Based on the quality assessment criteria, the ontology has been assessed in terms of the consistency and generality of the ontology description suggested by Gruber (1995) which also has been adopted in many other ontologies development research (Pak & Zhou, 2009; Sarantis & Askounis, 2009; Milton et al., 2012). Consistency of the ontology description refers to the absence of contradictory information regarding the class definition and their relationships. For example, the ontology has semantic consistency in the formal and informal definitions created and inferred in the

ontology. Building ontology in protégé has a key feature to process the ontology by a reasoner which checks the consistencies of the ontology definitions. The CISMET ontology has been executed using FaCT++ tableaux-based reasoner comes default with protégé to verify Description Logics (DL). The FaCT++ reasoner is applied in CISMET ontology to verify and ascertain the default tableau rules such as conjunction, disjunction, existential quantification, value restriction, negation, clash rules. It computes the class hierarchy into inferred hierarchy to automatically verifies the logical consistency of the ontology description. If a class has found to be inconsistent with its descriptions and relations with other classes, the name of the class will be highlighted in red color. The execution of FaCT++ reasoner verifies the ontology with no inconsistencies in its definitions.

Generality of the ontology description refers to the reusability of the ontology elements for various purposes within the same domain. The reusable ontology provides an unambiguous basic set of vocabulary which can be shared by some other process or applications development within the domain. The ontology for regulatory requirements compliant system development is developed based on existing ontologies in information system domain (Table 5). Furthermore, the generality of the ontology description also indicate that it defines 'is a kind of' relationships between the super class and subclass in a class hierarchy. The general classes in the ontology always have instances to specify the general description of the class hierarchy and the classes which cannot be instantiated by any instances is essentially not a general class in the ontology. In the ontology, the general class has different level of subclasses in the hierarchy and every class in the class hierarchy may have instances to specify the class descriptions.

Furthermore, the ontology has also been assessed based on the Relationships Richness (RR) and Attribute Richness (AR) metrics to show its usefulness (Mazzola et al., 2016). The Relationship Richness (RR) defines the ratio between number of relationships (P) defined in the ontology, divided by the sum of the number of subclasses in the class hierarchy (SC) which is same as the inheritance i.e., *'is a kind of'* relationships between superclass and subclass and the number of relationships (P) of the ontology. The RR metric reflects the diversity of the relationships in the ontology that contains many relations among various classes in the ontology rather than only superclass-subclass relationships. For example, if the RR value of an ontology is close to zero that indicates most of the relationships made in the ontology are mainly inheritance (i.e., the relations between subclass and superclass). On the other hand, if the RR value of an ontology is close to one that indicates there is almost no relationships between the classes as inheritance (i.e., no relationships between subclass and super class).

$$\mathrm{RR} = \frac{|\mathrm{P}|}{|\mathrm{SC}|+|\mathrm{P}|} \qquad \mathrm{AR} = \frac{|\mathrm{ATT}|}{|\mathrm{C}|}$$

The RR value of CISMET is 0.6, which implies high relationship richness of the proposed ontology, almost similar to other ontologies (ISD ontology has RR value 0.57 and Maintenance ontology has RR value 0.65) in the information system domain. Attribute Richness (AR) defines the average number of attributes/properties per class in the ontology which is calculate as number of attributes or properties for all classes (ATT) divided by the number of classes (C) in the ontology. The high AR value indicates more information about the ontology classes to describe the concepts. Table 5 shows the number of attributes/properties and classes in the ontology that has the high AR value 0.71 which is similar or better compared to some other ontologies (ISD ontology has AR value 0.62 and Maintenance ontology has AR value 0.41) in the information system development domain. These measures are not intended to act in a direct competing comparison, since the concepts in the various ontologies are complementary and can be combined (as also is done in the CISMET ontology), but they can serve as indications that the design and concepts of CISMET ontology is very close to the norm of the field.

4.5 Usefulness Evaluation of the Ontology

One of the main objectives of ontology development is to represent the interconnected knowledge so that it can be exploited for answering various queries. The usefulness evaluation process involves in taking an ontology of defined concepts and a set of documented texts describing a particular domain. The documents are then used in populating the ontology instances from the texts, and for identifying if the ontology returns correct/incorrect instances refereeing in the texts regarding the particular queries made in the ontology (Gómez-Pérez 1995; Hartmann et al., 2004). The usefulness evaluation of the ontology is made by implementing the recently enacted GDPR regulation into the CISMET ontology which imports several ontologies to describe the regulatory requirements compliant system development. Here, the instantiation of the concepts found in GDPR have been mapped to the EGRRC ontology classes in order to create the framework's description of regulatory requirements compliant CISMET ontology. Furthermore, the DLquery functions of the protégé tool has also been used in this study to present relevant queries and their results in Figure 61-65 mentioned in the introduction section. The queries have been built by the class properties following the object classes explained in the ontology triple descriptions. This can aid the involved information system researcher and system developer to understand how the newly introduced GDPR legislation affects them and what actions are needed from their side as part of their positioning in the operational chain of the information system development.

What are the system development goals referenced in the regulations to be implemented in the information system development?

In Figure 61, the following queries related to system development goals (along with their results) are presented: (A) what are the system development goals referenced in

GDPR regulation? (B) who are in control of pursuing the fulfillment of these system development goals?

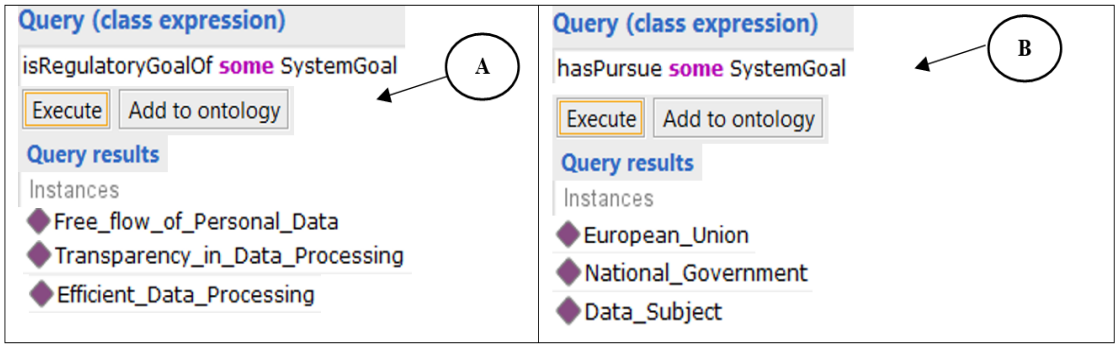


Figure 61: Query Results of System development Goals

The system development project may identify several goals of processing personal data which may not contradict with the GDPR regulation such as sharing the personal data among the EU member states and other countries freely without violating the data owner's rights and provides transparency in processing other's personal data over electronic media. Also, electronic processing of personal data makes them easily accessible whether the data dispersed on centralized or decentralized geographic locations. The GDPR regulation also provides the stakeholders who has the rights to pursue the fulfilment of the goals of the system development are the European Union (EU) who may support finically in various system development projects across the EU countries, the National Government who also provides financial support in the national e-service development projects, and the Data Subject are the citizens who provide their personal information to be used in the system.

What tasks are referenced in the regulation that describe the system development process?

In Figure 62, the following queries related to system development process (along with their results) are presented: (A) In GDPR regulation, what system maintenance tasks may enhance the system functionality but not required to perform? (B) what maintenance works become obliged by the GDPR regulation to perform in the system operation in case of any errors or malfunctioning?

The maintenance works regarding the system enhancement suggested by the GDPR regulations are as follows: The system may include and modify functions like charge reasonable fees for every service request of processing personal data, also specify a format of any information exchange in case of sharing the personal data, submit an electronic compliant beside the manual submission which may include in the system operation but not required.

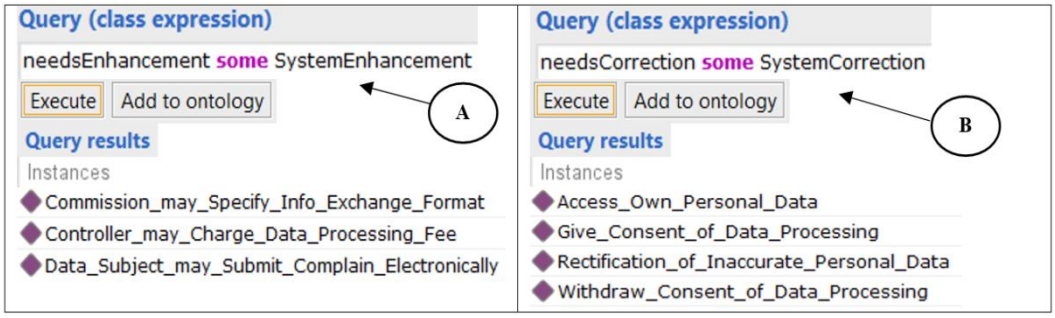


Figure 62: Query Results of System Development Process

On the other hand, the system maintenance tasks regarding any errors in the system functionalities like information access, update, delete request of personal data by the data subjects, also their rights to give and withdraw consent of processing personal data becomes obligatory compliance in the system operation and maintenance by the GDPR regulation.

What system services are affected by the regulations?

In Figure 63, the following queries related to system services (along with their results) are presented: (A) what are the regulatory requirements for Data Services referenced in the GDPR regulation? (B) which service needs private data in its operations? (C) who are the authorized system users to access those services? (D) what roles are responsible to provide services to the system users?

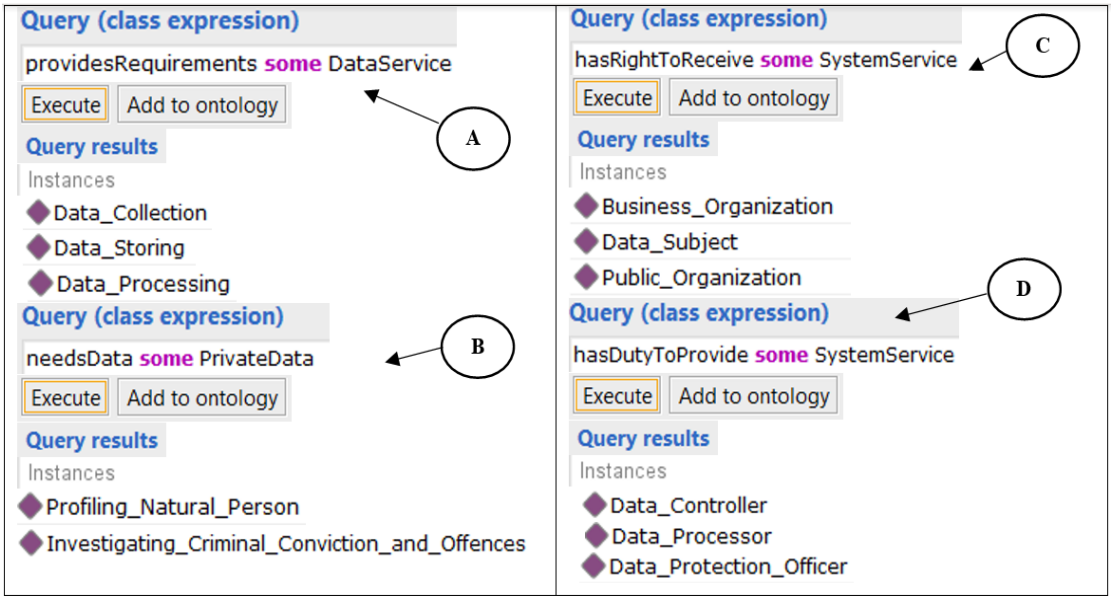


Figure 63: Query results of the services provided by the system.

There are many regulatory requirements for data service in the GDPR regulation such as Data Collection to collect personal data from the data subject, Data Storing records data in the storage media, Data Processing processes the data to retrieve useful information, etc. The personal data are needed in the services like profiling the natural

person to monitor the employees regarding their performance at work as well as identify their behavior, health and economic condition, interest and reliability in making decision to assign suitable tasks. Also, personal data can be used in criminal conviction investigation to measure public security threats. GDPR has also authorized several users to access personal data are the Data Subjects who are the owner of the personal data have the right to access their own data, the business organizations who may use the personal data for direct marketing based on the consent given by the data owner, and the Public Organizations may require the personal data for investigating any criminal offences in the country or pursue any statistical and scientific research. The GDPR regulation also defines the responsible roles for providing the data services are the data controller who determines the data processing purposes and means based on the regulations, the data processor who actually processes the personal data based on the user requests, and the data protection officer advises the impact assessment of data protection laws and regulations.

What resources are referenced in the regulation to be used in system development?

In Figure 64, the following queries related to the system resources (along with their results) are presented: (A) what private data referenced in the GDPR regulation are used in the system services and maintenance activities? (B) what software application or tools and hardware devices are imposed to be used in the system operation by the GDPR regulation?

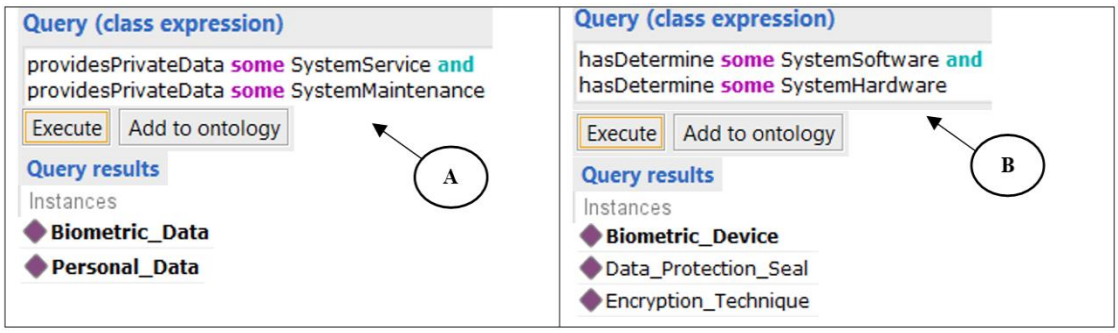


Figure 64: Query results of resources in the system development

The GDPR regulation references the private information given by the citizens as the personal data to be protected from any unauthorized access, also the biometric data resulting from a biometric device to confirm any person's identification uniquely in requesting and processing personal data in the system operations. Furthermore, the GDPR regulation defines some software applications and hardware devices to be used in the system operation for processing personal data, such as the use of data encryption and decryption techniques in the transaction of personal data, and the data protection seal attached to the processed copy of personal data showing the compliance of the data processor in personal data processing with the enacted regulations. And, the biometric device is used in the system operation to produce biometric data in order to identify a person.

What system activities referenced in the regulation are permissible and restricted to be performed?

In Figure 65, the following queries related to system/project activities (along with their results) are presented: (A) what are the project development activities referenced in the GDPR regulation? (B) what are the triggering events in performing the system activities? (C) what constraints are placed by the GDPR regulation in performing the system activities?

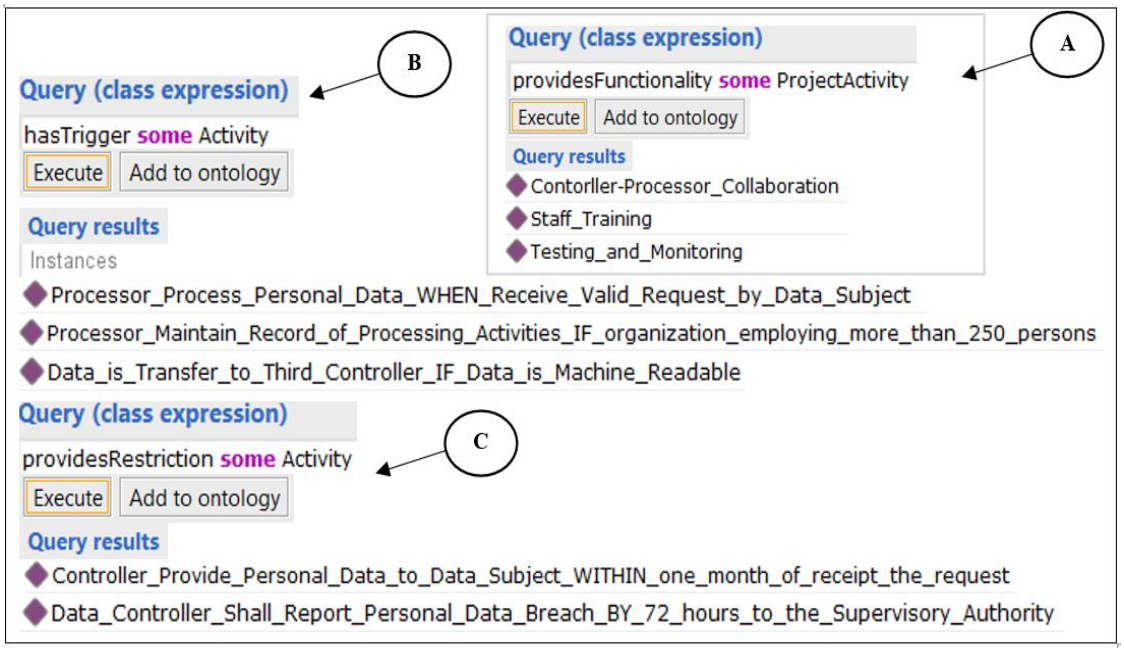


Figure 65: Query results of system activities

The GDPR regulation describes various project management activities in the system development such as the data controller and processor collaboration in personal data processing, regular testing and monitoring in measuring the effectiveness and security in data processing, staff training in raising data protection awareness. Furthermore, The GDPR regulation describes the triggering events of performing the system activities such as the data processor process personal data when they receive a valid data processing request by the data subject, the data processor will maintain the data processing records only if the data subject's organizations have more than 250 employees, the data will be transferred to any third countries only if the data is in machine readable format. Furthermore, the GDPR regulations also impose time restriction on human resource in performing activities such as within 1 month of receiving data subject's request for accessing their personal data the data controller shall provide the data to them. Also, for any personal data breach the data controller shall notify the supervisory authority by 72 hours.

4.6 Enhanced End User Interface Usage of the Ontology

Generally, the users are not often very familiar and have expertise with the query languages. Therefore, in order to enhance the usability such as the way CISMET and its backend implementation is offered to the end-user interface, a relevant software application has been developed, that aims to demonstrate the guidance of the system developer towards the goal of creating a regulatory compliant information system. The application also serves with the results of various queries (Figure 66-71) regarding the modifications around technical aspects of the IT system development while adapting the legislative actions on the system development components. For example, the IT system developer wants to know what are the specific regulatory requirements for the data services and authentication services in order to fulfill the rights of the data subject and to be compliant with the enacted regulation? The query and its results are shown in the Figure 66-68.

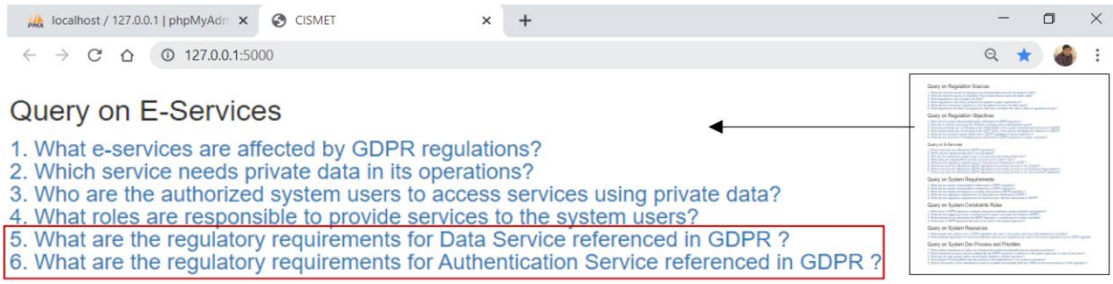
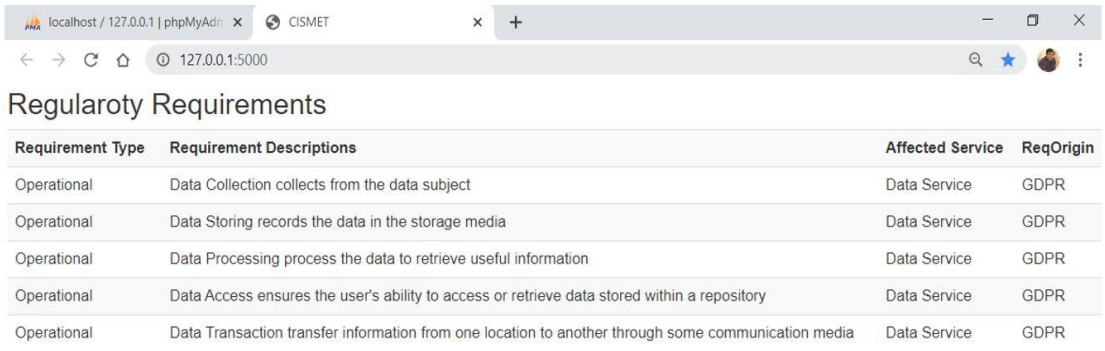
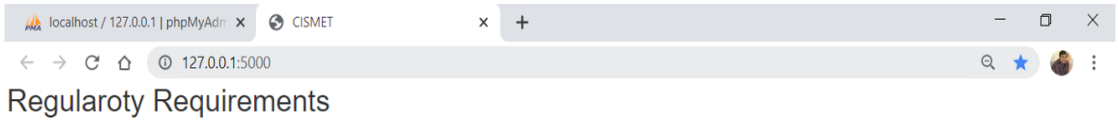


Figure 66: Some of the queries to guide IT system developer



Requirement Type	Requirement Descriptions	Affected Service	ReqOrigin
Operational	Data Collection collects from the data subject	Data Service	GDPR
Operational	Data Storing records the data in the storage media	Data Service	GDPR
Operational	Data Processing process the data to retrieve useful information	Data Service	GDPR
Operational	Data Access ensures the user's ability to access or retrieve data stored within a repository	Data Service	GDPR
Operational	Data Transaction transfer information from one location to another through some communication media	Data Service	GDPR

Figure 67: Part of the query results of regulatory requirements for Data Service



Requirement Type	Requirement Descriptions	Affected Service	ReqOrigin
Operational	Data controller shall use public key cryptography in processing and sharing private data	Authentication	GDPR
Operational	Biometric authentication may use by the data subject to give consent of processing their personal data	Authentication	GDPR
Operational	Data controller and processor are required to perform a Data Protection Impact Assessment (DPIA) prior to data processing	Authentication	GDPR

Figure 68: Part of results of regulatory requirements for Authentication Service

Moreover, apart from the list of queries presented in the application, the latter also allows the system developer to search for specific results about various queries regarding the regulatory compliant IT system development. For example, what are the constraints made upon the data controller by the GDPR regulation in processing personal data? What is the priority of the maintenance tasks of a system functionality that unintentionally allows unauthorized access of encrypted data? The queries and its results are demonstrated in Figure 69 and 70.

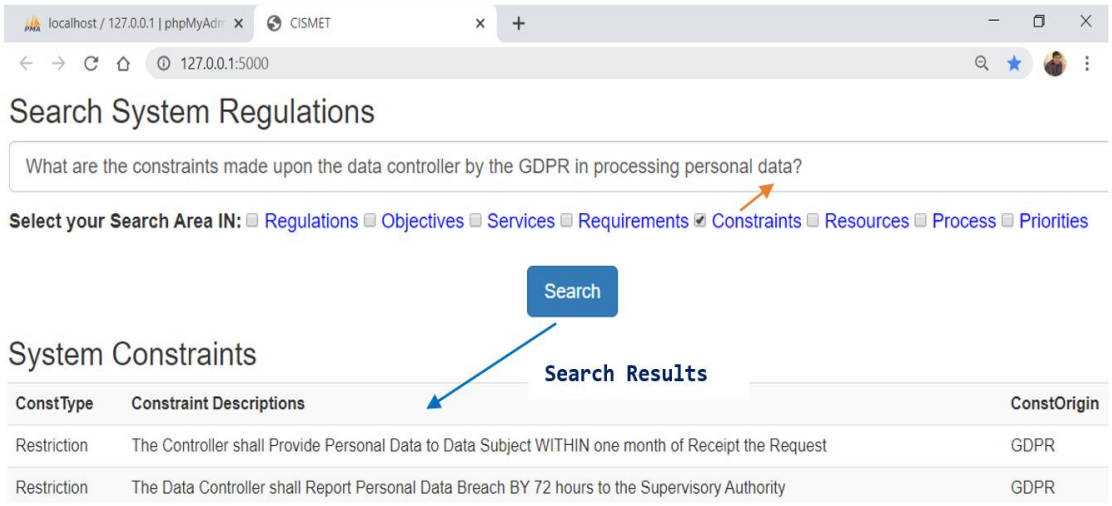


Figure 69: Search results of query made in resource constraints

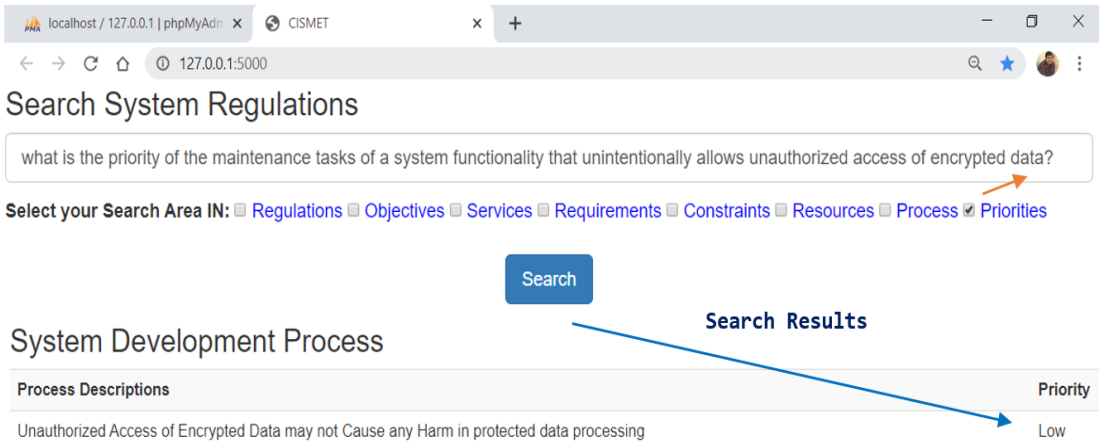


Figure 70: Search results of query made in priorities of system functionalities

Furthermore, one of the most useful feature of this application is that it allows the IT system developer to write system specification in it and verify with the existing regulations in order to validate the system functionalities for the regulatory requirements compliance. For example, if the service provider needs to transfer personal data to third counties in providing cloud service then is it allowed by the enacted regulations and with what restricion or condition it is permitted to transfer is shown in Figure 71.

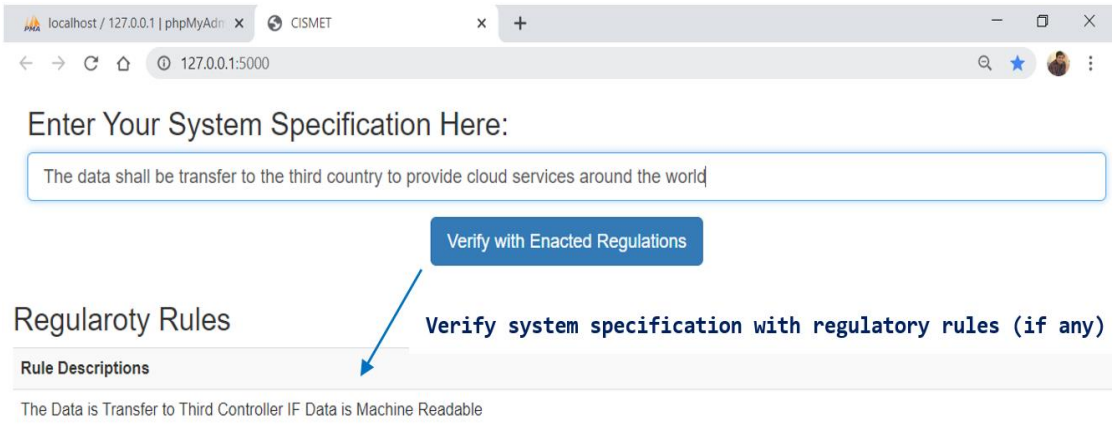


Figure 71: Verify the system functionalities with existing regulations

The application also allows the system developer to insert, update or delete the instances of the ontology class components based on the enacted regulations from various authorities, as shown in Figure 72.

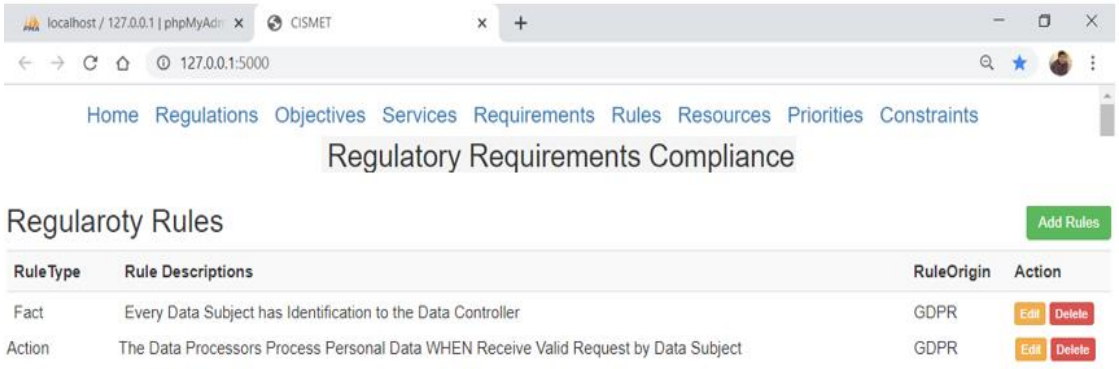


Figure 72: CRUD operation of Regulatory Rules in the application

Furthermore, the application provides only the potential regulatory rules (if any) that needs to be followed in the system development specification, however, how the rules may affect the system specification is often not easily identifiable or obvious to the system developer when deciding probable compliance of the regulatory rules with the system specifications. Therefore, a pseudo-code has been generated to help the IT system developer to understand and deduce conclusions about the compliance of their system specification with the enacted regulatory rules extracted from the application. A set of questions has been generated based on the ontology description that can be placed in the conditions presented in the pseudocode to extract decisions regarding the compliance of the regulatory rules to the IT system development specification (Table 7). Here the users reply to the questions and a final compliance check decision is returned to them. Having a pseudocode to model the final compliance has been used as an easy way to link between legal concepts and the IT implementation, a kind of summary of the legal knowledge that can then be forwarded to a developer for more abstract implementations (Corrales et al, 2019; Barnitzke et al, 2011).

Table 7: Questions and Pseudo-code of Regulatory Requirements Compliance

RRC01: Do you need to develop/maintain your system based on the regulations?
RRC02: Do you need to identify regulatory rules for your system development or maintenance tasks?
RRC03: Does the system have obligatory rules which must be considered when providing system services?
RRC04: Does the rule define the fulfillment of the rights of the service users and other stakeholders?
RRC05: Does the system specification covers a simple rule which has only single clause or condition?
RRC06: Does the system specification covers a compound rule (i.e., multiple conditions in the rule with AND/OR operator joining them)?
RRC07: Does the system specification covers whole of a compound rule (i.e., cover all the conditions presented in the rule)?
RRC08: Does the multiple conditions combined with AND operator (i.e., two or more conditions on system specification joined with AND where each of the condition must be complied}?
RRC09: Does the rule considered to be an option to be implemented in the system operation which may not require in the system operation?
RRC10: Does the rule have dynamic status (i.e., open for interpretation) to be decided in system operation?

PSEUDO-CODE of making decision of the regulatory requirements compliance

```
if (RRC01 == True)
{
  if (RRC02 == True)
  {
   if (RRC03 == True OR RRC04 == True)
   {
     if (RRC05 == True OR RRC06 == True)
     {
       if (RRC07 == True)
       {
         Decision Reached: Regulatory Requirements Compliance == TRUE
       }
     }
     else if (RRC07 == False)
     {
       if (RRC08 == True)
       {
         Decision Reached: Regulatory Requirements Compliance == FALSE
       }
     }
   }
```

```
    else if (RRC03 == False OR RRC04 == False OR RRC08 ==  True OR RRC09 == True)
    {
       Decision Reached: Regulatory Requirements Compliance == TRUE
    }
   }
}
```

4.7 Remarks on CISMET Ontology

For the conceptualization of regulatory requirements compliant CISMET ontology, a review of existing literature has been performed. From the literature review of existing ontologies in information system domain, a total of 35 class concepts have been extracted and presented in Table 5 that describe the core concepts of information system development in CISMET ontology. The classes are then organized in an ontology class hierarchy which has 6 parent classes that describe the goal of the system development, system services, system artifacts, system development process, system development activities, and resources to perform the system operation and project activities. There are 29 subclasses derived from the parent classes that describe the specific properties and instances of the CISMET ontology. There are 25 class properties have been derived from the literature review and this class properties have been used to define 44 class relationships between the EGRRC class entities with CISMET ontology to describe the instances of information system development projects based on the regulations. Furthermore, the relationship richness and attribute richness metrics show that the ontology has diversity of relationships and presents more information in describing the concepts in the ontology. Moreover, a total of 13 relevant queries along with their results have been presented to demonstrate the usefulness of the ontology.

The CISMET ontology could be applied in the three example case organizations such as ChoicePoint, Tricare, and Stanford Hospital discussed in section 1.3. These three organizations were given such expensive consequences for not being compliant with some of the enacted regulations and policies such as Fair Credit Reporting Act (FCRA) enacted by United States Federal Government legislation to promote fairness, accuracy, and privacy of personal information contained in consumer reporting agencies, Health Insurance Portability and Accountability Act (HIPAA), etc. It can be assumed that the organizations of the above examples had ambiguous understanding of the regulations and difficulties in inferring the regulatory requirements from various enacted regulations in managing compliance related tasks in their information system development. In these three example cases (ChoicePoint, Tricare, and Stanford Hospital) the regulation document texts (e.g., FCRA, HIPPA) could be mapped in populating the instances of the CISMET ontology classes and create the ontology framework descriptions. And relevant query results could aid the involved stakeholders in these three organizations to understand how the implemented

legislation (e.g., FCRA, HIPPA) could affects them and what actions were needed from their side as part of their positioning in the regulatory compliant information system development. For example, Figure 73 shows (A) What regulatory requirements could be implemented in providing data services? (B) What restrictions could be implemented in the organizations in protecting private data?

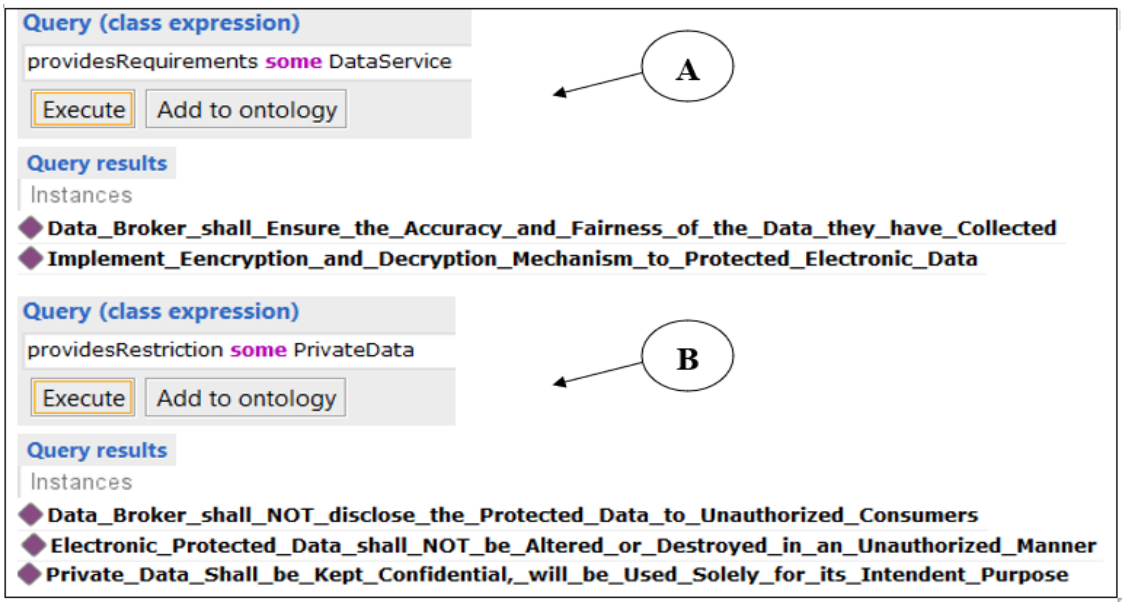


Figure 73: Query Results of Requirements and Restrictions on Data Services

The regulatory requirements for data services that could be included in the system development of the example case organizations are ensuring the data accuracy and fairness while collecting and processing the data (FCRA, Rule No. 602), Also, the organizations could implement encryption and decryption mechanism to protect the confidential data stored and processed over electronic media to guard them against any unauthorized access (HIPPA, 164.312(e)(2)(ii)). Furthermore, the restrictions regarding private data processing that could be implemented in the system development of the example organizations cases are the data processor shall not disclose the protected private data to any unauthorized users (FCRA, Rule No. 605A). And the private confidential data needs to be preserved only for its intended use (FCRA, Rule No. 604). Also, the electronic form of the protected data shall not be altered or destroyed without the authorizations of that particular operations (HIPPA, 164.312(c)(2)).

Chapter 5: Discussion and Conclusion

"Research is the process of going up alleys to see if they are blind."

- Marston Bates

This section discusses the summary of the research works such as existing challenges regarding research/practice in the field of E-Government system development and contribution of the research works with its innovation and evolution process. Also, discusses the design rationale to present the research decisions taken in this thesis. Furthermore, this section also discusses the limitations address by this study and related recommendations for the future works.

5.1 Review and Discussion on Achievements

Along with the advancement of E-Government initiatives across various parts of today's world, significant challenges become obvious to be considered in the E-Government service development. And the regulatory requirements compliance remains the primary challenge of the E-Government system development as policy and regulations are growing and changing regulatory landscape environment from multiple authorities (OECD, 2020). The initial aim of this research was set out to investigate and analyze the E-Government policy and regulations to provide an overview and understanding about regulatory requirements compliance of the E-Government system development. And identify the implications of regulatory requirements compliance in a successful project of the E-Government information system development (Figure 74).

In E-Government system development the E-services are often closely controlled with existing and/or upcoming regulatory frameworks. As a result, the E-Government system development projects have a significant need for compliance with the increasingly growing regulations. However, how a legislation may or may not affect the E-Government information system development project is often not easily identifiable or obvious due to the lack of a framework that provides comprehensive guidelines to understand the concepts and include actions related to the compliance of regulatory requirements in the system development process. Furthermore, due to the frequent update of legislative content, either in local, regional, or wider level (e.g., EU level), these aspects need to be identified clearly and their effects be understood in the various levels of E-Government system development process. Hence, the research addresses the following key challenges in the E-Government information system development projects:

- Inadequate understanding of the regulatory requirements compliance in the E-Government system development.

- Frequently update of legislative contents for E-Government system services.
- Lack of a comprehensive framework that organize, structure, and describes the interlinked concepts of regulatory requirements compliance in E-Government system development.
- Domain gap between the legal science, E-Government, and Information Technology (IT).

Therefore, the contribution of this research is then extended to introduce the EGRRC ontology framework that integrates the concepts of regulatory requirements compliance in the E-Government system development projects and discuss the implementation of the ontology in the recently enacted General Data Protection Regulation (GDPR) for personal data processing in EU member countries. In order to provide a clear understanding of the regulatory requirements compliance in the E-Government system development, the EGRRC ontology has been presented in Chapter 3 which organize, structure, and describes the interlinked concepts of regulatory requirements compliance in the E-Government system development. The EGRRC ontology framework discusses various sources of E-Government regulatory requirements among several types of regulations scattered in local, regional, or wider level. The defined objectives and goals of the regulations and various types of regulatory requirements to properly identify those and implement in the E-Government system development. Also, discusses various types of E-Government services affected by the regulations and the formulation of regulatory rules in the requirements to clearly understand their components and associations in the E-Government system development. Furthermore, the EGRRC ontology also describes the prioritization and maturity of the E-Government regulatory requirements as every requirements do not have the same level of priority to be compliant in the E-Government system development and sometimes needs additional modifications as a result of the evolution of regulatory requirements in the amended regulations.

Furthermore, in order to bridge the gap between legal science, E-Government, and IT, this study further integrates the concepts of E-Government regulatory requirements compliance (EGRRC ontology) to the information system development process (CISMET ontology), thus bridging these three domain. The study proceeds with the use of entities defined in the EGRRC ontology and combined with the core concepts of CISMET and links them together in order to assist in the detection of compliance related tasks and actions needed in parts of the E-Government system development project such as E-Government system goals, services, artifacts, process, activities, and resources needed in the project development based on the enacted regulations. Finally, this allows the E-Government system developer with the opportunity to make various queries about the effects of the legislation in the E-Government information system development projects through the implemented existing example legislations (such as GDPR) or their future extensions into the integrated ontology framework. For this reason, a specialized front-end application is also presented that can aid in formulating and submitting these queries.

In the previous decades, there were many regulations enacted to control the traditional government operations and service delivery to the citizens and business organization. However, due to the transformation to the digital world of electronic services, many challenges become a significant barrier towards the growth of E-Government revolutions. For instance, the privacy and security concerns of collecting, recording, processing, and transferring individual's confidential personal information becomes one of the key issues to revise the earlier regulations. The data protection regulations are rapidly evolving to enforce its impacts on how the organizations should approach the data storage and provide protection of data against the data breach, produce notification of the incidence of data breach, implementing cybersecurity for data transactions, etc. For example, the European Commission has presented the new GDPR regulation enacted on 25 May 2018 which is planned to replace the old Directive 95/46/EC 1995. The newly formed GDPR constitutes the legal framework for personal data processing in the EU countries. The GDPR is presented not only to harmonize data privacy laws across Europe in protecting the rights of using individual's personal data but also to facilitate the freedom of exchanging personal data within member states of European Union through a uniform legislation towards advancing the digital agenda and economic growth across EU countries.

Therefore, he General Data Protection Regulation (GDPR) has been implemented in the EGRRC and CISMET ontologies to demonstrate the results of the queries. Nonetheless, some other regulations or the amendment or extension of an existing regulation can also be implemented in the EGRRC and CISMET ontologies to demonstrate the ontology query results based on that regulations. The regulation document texts can be used and mapped in populating the instances of the defined ontology classes and create the ontology framework descriptions. And relevant queries can be demonstrated to present the results of the queries that can aid the involved stakeholders to understand how the implemented legislation affects them and what actions are needed from their side as part of their positioning in the system development process.

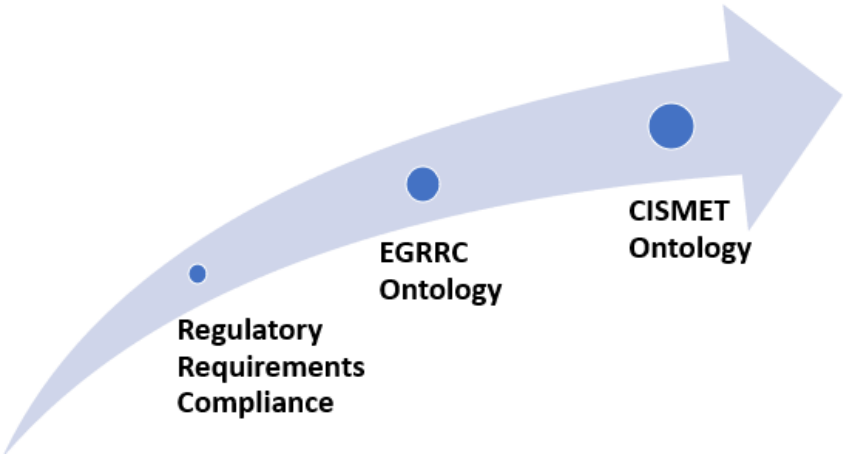


Figure 74: Evolution of the Research Contribution

The Design Science Research Methodology (DSRM) is generally adopted in this study as a research paradigm where the EGRRC and CISMET ontologies have been introduced, demonstrated, and evaluated for solving the existing challenges and problems regarding regulatory requirements compliance in the E-Government system development (Figure 75). The DSRM has been used in several research in information systems domain to propose and evaluate various research outcome. It provides a nominal process model for doing research and also provides a mental model for presenting and evaluating solutions of the research (Hevner & Chatterjee, 2010; Peffers et al., 2007; Peffers et al., 2006).

The motivation and research questions of this study have been drawn as a consequence of the challenges and problems regarding high risk of non-compliance with the regulatory requirements in E-Government system development because of the research gap of interconnecting various concepts belonging to legal, government-administrative, and IT domain. As a solution to this problem, the objective of this study is to introduce the EGRRC and CISMET ontology framework that describes the interrelated concepts of regulatory requirements compliance in legal, E-Government, and IT domain. This also serves the E-Government system analyst with the results of various queries regarding the concepts of E-Government services and modifications around technical aspects of the system development while adapting the legislative actions on the E-Government information system development components.

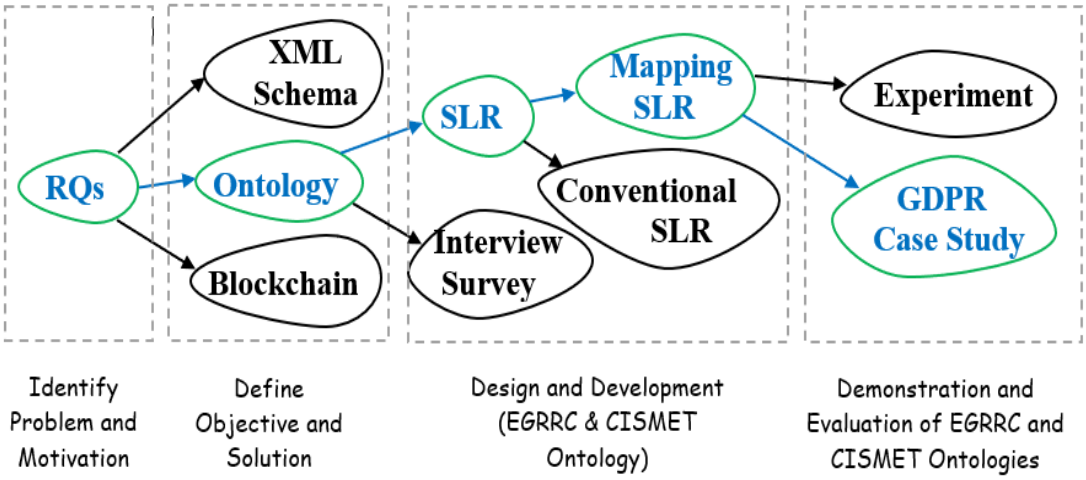


Figure 75 : Research Design Rationale

To serve the purpose of this study there are several methods that can be used for knowledge representation in various application domains. Such as an XML schema can be used to describe the structure of a legal document that can be machine-understandable and automatically processed for meeting legal requirements in a system development. A blockchain approach can be used in creating and administrating smart contracts for a system development to record and represent the information in a contract or policy in such a way that is difficult to alter by unknown authorities. However, both XML schemas as well as blockchain approaches, while

feasible to be used during runtime of the system operations, they cannot efficiently capture dependencies between concepts during the design time in order to guide developers, nor leverage inference capabilities based on the concept structure. Hence, the OWL ontology has been chosen to present the solution of this research. It describes the existing concepts from the domain (e.g., legal, government-administrative, and IT) in order to enhance the reusability and extension of descriptions. Furthermore, ontology is a widely accepted knowledge representation paradigm in several application domains and becoming popular in the E-Government system development domain in knowledge management and representation. Additionally, ontology is an essential tool for knowledge representation in establishing interconnection between cascading concepts among various domains with well-defined terminologies, definitions, and their interrelationships (Yang et al., 2019; Kendall & McGuinness, 2019).

For the purpose of design and development of the EGRRC and CISMET ontology, Systematic Literature Review (SLR) particularly the mapping category of SLR has been employed in this study to review the related existing works on legal, E-Government, and IT domains in order to enhance the reusability and extension of descriptions in the EGRRC and CISMET ontology for regulatory requirements compliance in E-Government information system development. The mapping SLR is particularly more suitable to meet the objective of this research because this study undertakes a conceptual analysis of various issues presented in the literature regarding legal, E-Government, and IT domains where conventional SLR and interview/survey methods primarily provides quantitative results and comparisons of statistical data analysis (Kitchenham et al., 2010; Petersen et al., 2008).

Finally, to demonstrate and evaluate the proposed EGRRC and CISMET ontology, the case study approach has been followed in this research where the General Data Protection Regulation (GDPR) is implemented in the proposed EGRRC and CISMET ontology to demonstrate the results. Among some other research methods such as experiments, the case study approach is more suitable in this research context where a case study provides the researcher with a descriptive qualitative method to explore the subject matter to generate a multifaceted and in-depth understanding about a particular issue. On the other hand, an experiment method is unlike the case study is an empirical approach with a quantitative research method which primarily provides results from the statistical data analysis to test a given hypothesis (Kumar, 2018; Mishra & Alok, 2011).

5.2 Limitation and Future Research

"No research is ever quite complete. It is the glory of a good bit of work that it opens the way something still better, and this repeatedly leads to its own eclipse."

- Mervin Gordon

This study addresses the following limitations and recommends for potential future research. For example, the regulatory documents are very often consisting of a large document that covers many issues and rules where all of the directives might not be related and applicable in the system development projects. Furthermore, the analysis of regulation documents might often need some level of expertise in legal science in populating the instances of ontology class entities. Therefore, it would be useful to automatically instantiate the ontology classes from the regulatory documents using Natural Language Processing (NLP) of the regulation text. Moreover, many of the policies and regulations are often written in native languages in various countries where NLP can also be useful in translating the regulatory documents and instantiate the ontology classes accordingly. This might become easier and faster for the system developer or related stakeholder to identify the regulatory requirements and its compliance in the E-Government and Information system development projects.

Another extension of this research can be annotating the system/software components or services with the concepts from EGRRC and CISMET ontologies (e.g., regulatory rules, requirements, services, goals, activities, resources, artifacts, etc.). This way, when a developer includes a component or service in their system/software application (i.e., design level or code level), the regulatory compliance related issues would be stemming or inferred from this concept can be automatically detected from the EGRRC and CISMET ontologies and communicated to the developer of an actual system/software implementation.

A potential high-level process workflow of the idea of annotation mechanism is sketched in Figure 76 which generally shows the abstract process of inferring regulatory knowledge about a component or services in the system/software design/coding elements. Here, the annotation mechanism can start with the extraction process of the class properties (i.e., concepts of the class hierarchy and their interrelations) and instances of the classes from EGRRC and CISMET ontologies. These class properties and instances can be further used for identifying various concept keywords and related class instances regarding the regulatory knowledge and stored in a database. Then, the database can be integrated with the process of system development to be matched with the system design or coding elements. The corresponding regulatory compliance issues regarding system design/coding elements would be then communicated to the UML diagram and system source code.

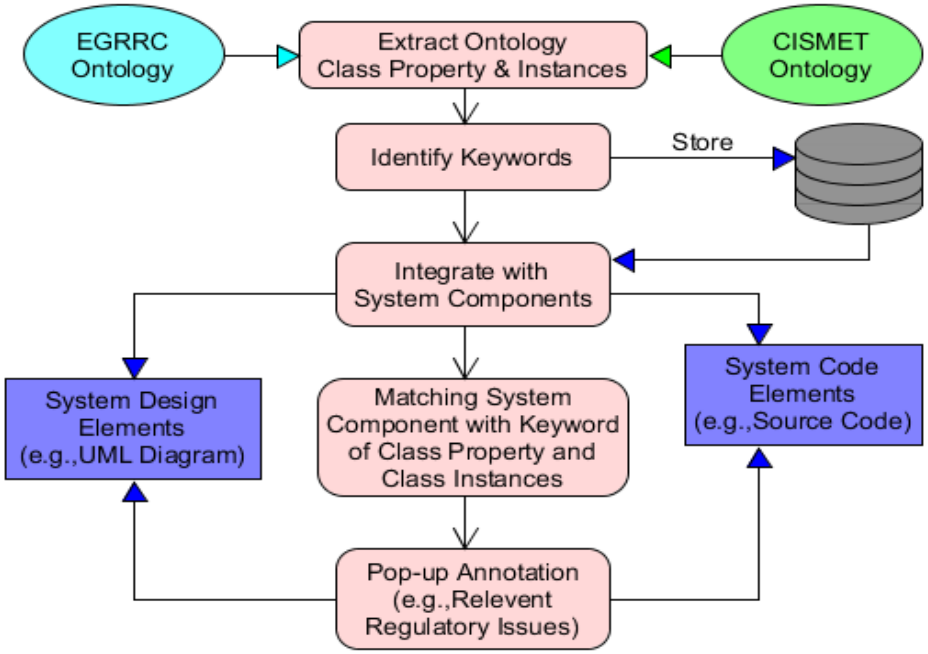


Figure 76: Annotation Mechanism of System Components

In Figure 77, examples have been presented regarding the potential annotation message appeared in the system UML design activities that can be considered while designing the system/software components. Also, Figure 78 shows the example of the potential annotation message appeared in the source code snipped of the system or software development.

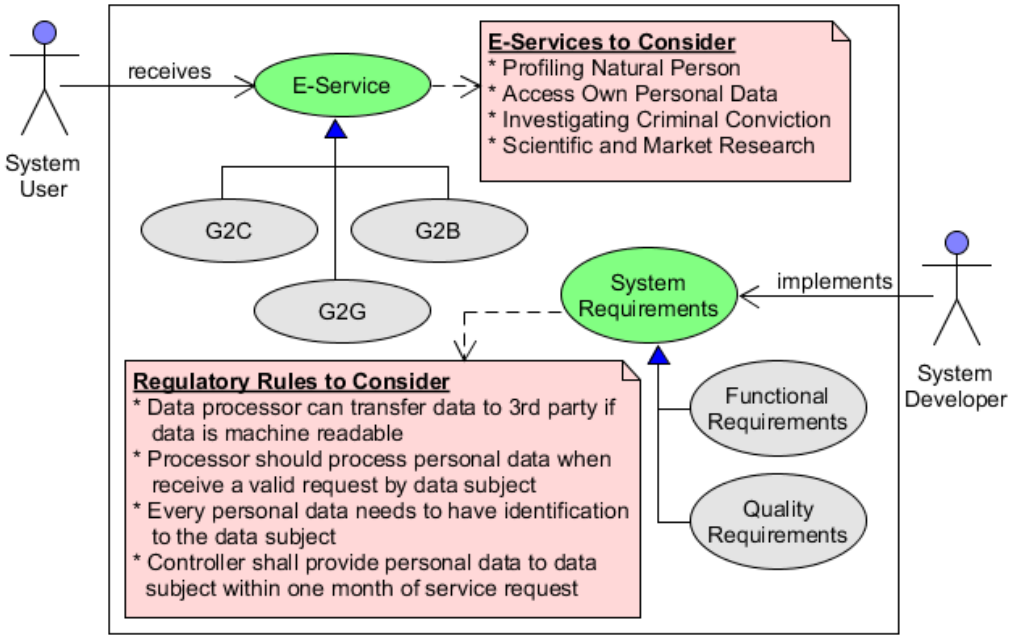


Figure 77: Annotation of System Component in Use case Design

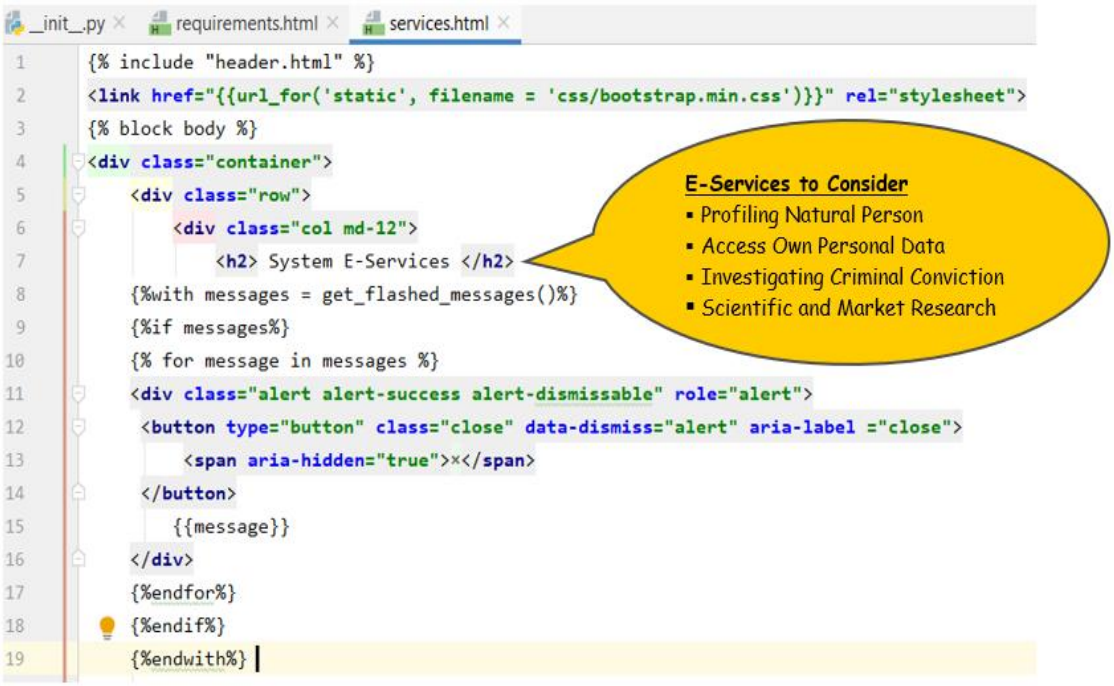


Figure 78: Annotation of System Component in Source Code Snippet

Here, the visualized and explicit annotation can communicate more details about the sophisticate issues regarding regulatory requirements compliance of developing the system components. This would be much more useful and efficient in providing explicit knowledge regarding regulatory requirements compliance rather than just implicitly highlighting or underlining the system component in a requirement specification document (Hwang et al., 2007). Furthermore, the annotation mechanism would be a useful technique to detect and understand additional new information regarding a component in a system/software application development (Glover et al., 2007). In this area, studies have shown some powerful effects of integrating the visualized and explicit annotation with the existing information that enhance the analysis and learning process of system/software application development. For example, Zarzour & Sellami (2017) present a linked data-based annotation system that allows to retrieve and enrich knowledge from linked cloud data. A collaborative annotation system is proposed by Chen & Chen (2014) that describe a framework of interactive discussion using annotation for improving the performance of thinking process and discussion of system components. A code annotation model is proposed by Yao et al. (2019) that generate annotations from natural language description to provide a better and semantic meaning for a given code snippet.

References

Abdullah, N. S., Sadiq, S. Indulska, M. (2010). Emerging challenges in information systems research for regulatory compliance management. In *Proceedings of the 22nd International Conference on Advanced Information Systems Engineering*. Hammamet, Tunisia.

Alasem, A. (2009). An Overview of E-Government Metadata Standards and Initiatives based on Dublin Core. *Electronic Journal of E-Government (EJEG), 7*(1), 1-10.

Alexopoulos, P., Kafentzis, K., Benetou, X., Tagaris, T. & Georgolios, P. (2007). Towards a Generic Fraud Ontology in E-Government. In *Proceedings of the 2nd International Conference on e-Business.* Barcelona, Spain.

Almarabeh, T. & AbuAli, A. (2010). A general framework for E-Government: definition maturity challenges, opportunities, and success. *European Journal of Scientific Research 39*(1), 29-42.

Alpar, P. & Olbrich, S. (2005). Legal requirements and modelling of processes in E-Government. *Electronic journal of E-Government, 3*(3), 107-116.

Al-rawahna, A., Salamh M., Chen, S., Hung, C. (2019). The barriers of e-government success: An empirical study from Jordan. *International Journal of Managing Public Sector Information and Communication Technologies, 9*(2), 1-18.

Al-Sayed, M. M., Hassan, H. A, & Omara, F. A. (2020). CloudFNF: An ontology structure for functional and non-functional features of cloud services. *Journal of Parallel and Distributed Computing 141*(2020), 143–173.

Amalanathan, A., Anouncia, S. M., Vairamuthu, S., Vasudevan, M. (2015). A Framework for E-Governance System using Linked Data and Belief-desire-intention Agent. *Indian Journal of Science and Technology 8*(15), 1-6.

Anadiotis, G. (2018). GDPR in real life: Fear, uncertainty and doubt. Available at https://www. zdnet.com/article/gdpr-in-real-life-fear-uncertainty-and-doubt, Accessed on 29 November 2018.

Angelis, F.D., Polzonetti, A. & Tapanelli, P. (2010). Policy makers and performance management in E-Government domain. In *Proceedings of the 4th International Conference on Theory and Practice of Electronic Governance*. Beijing, China.

Angelopoulos, K., Diamantopoulou, V., Mouratidis, H., Pavlidis, M., Salnitri, M., Giorgini, P., & Ruiz, J. F. (2017). A holistic approach for privacy protection in E-government. In *Proceedings of 12th International Conference on Availability, Reliability and Security*. Reggio Calabria, Italy.

Annamalai, G., Hussain, R., Cakkol, M., Roy, R., Evans, S., & Tiwari, A. (2011). *An Ontology for Product-Service Systems*. In *Proceedings of the 3rd International Conference on Industrial Product Service Systems*. Braunschweig, Germany.

Anon, J. L., Filowitz, H., Kovatch, J. M. (2007). Integrating Sarbanes-Oxley Controls into an Investment Firm Governance Framework. *The Journal of Investment Compliance 8*, 40–43.

Apostolou, D., Stojanovic, L., Lobo, T., Miró, J. & Papadakis, A. (2005). Configuring E-Government Services Using Ontologies. In Funabashi, M. and Grzech, A. (Ed.). *Challenges of Expanding Internet: E-Commerce, E-Business, and E-Government* (p.141-155). Springer US.

Bace, J., Rozwell, C., Feiman, J., and Kirwin, B. (2006). Understanding the Costs of Compliance. Technical Report, Gartner Research Inc.

Barnitzke, B., Ziegler, W., Vafiadis, G., Nair, S., Kousiouris, G., Corrales, M. Wäldrich O., Forgó N. & Varvarigou, T. (2011). Legal restraints and security requirements on personal data and their technical implementation in clouds. In *Workshop for E-contracting for Clouds, eChallenges* (pp. 51-55).

Barrett, K. Strassner, J., van der Meer, S., Donnelly, W. Jennings, B. & Davy, S. (2007). A policy representation format domain ontology for policy transformation. In *2nd International Workshop on Modelling Autonomic Communications Environments*. Niagara Falls, Canada.

Bastos, E. C., Barcellos, M. P., & de Almeida Falbo, R. (2018). Using semantic documentation to support software project management. *Journal on Data Semantics*, *7*(2), 107-132.

Bekkers, V. (2009). Flexible information infrastructures in Dutch E-Government collaboration arrangements: Experiences and policy implications. *Government Information Quarterly*, *26*(1), 60-68.

Beydoun, G., Low, G., García-Sánchez, F., Valencia-García, R., Martínez-Béjar, R. (2014). Identification of ontologies to support information systems development. *Information Systems Journal 46*, 45-60.

Bianchini, D., De Antonellis, V., Pernici, B., & Plebani, P. (2006). Ontology-based methodology for e-service discovery. *Information Systems*, *31*(4-5), 361-380.

Bizer, C. (2009). The emerging web of linked data. *IEEE intelligent systems*, *24*(5), 87-92.

Boella, G., Janssen, M., Hulstijn, J., Humphreys, L., Van Der Torre, L. (2013). *Managing legal interpretation in regulatory compliance*. In *proceedings of the 14th International Conference on Artificial Intelligence and Law*, ACM.

Braganza, A. & Franken, A. (2007). SOX, Compliance and Power Relationships. *Communi-cations of the ACM 50*(9), 97-102.

Breaux, T. D. (2010). A method to acquire compliance monitors from regulations. In *the 3rd International Workshop on Requirements Engineering and Law.* Sydney, Australia.

Breaux, T. D. & Anton, A. I. (2008). Analyzing Regulatory Rules for Privacy and Security Requirements. *IEEE Transactions on Software Engineering, 34*(1), 5-20.

Breaux, T. D., Vail, M. & Anton, I. (2006). Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations. In *Proceedings of the 14th IEEE International Requirements Engineering Conference.* Saint Paul, USA.

Campbell, G. A. (2006). *Ontology stack for a policy wizard*. Department of Computing Science and Mathematics, University of Stirling, Scotland.

Charalabidis, Y., Loukis, E., Alexopoulos, C., & Lachana, Z. (2019). The Three Generations of Electronic Government: From Service Provision to Open Data and to Policy Analytics. In *International Conference on Electronic Government*. Linköping, Sweden.

Chen, C. M., & Huang, S. H. (2014). Web-based reading annotation system with an attention-based self-regulated learning mechanism for promoting reading performance. *British Journal of Educational Technology*, *45*(5), 959-980.

Cherouana, A., Mahdaoui, L., Bellatreche, L., & Medjahed, B. (2019). A semantic approach for generating government processes. *International Journal of Web and Grid Services*, *15*(1), 59-92.

Chiriac, L. & Szabo, Z. K. (2014). Legal and Regulatory Implications of the Successful Implementation of the Public Policy of e-Gov in Romania Reflection on the Future and Barriers. *Juridical Current*, *17*(3), 87-100.

Chun, S. (2019). E-commerce liability and security breaches in mobile payment for e-business sustainability. *The Journal of Sustainability, 11*(3), 1-18.

Cleven, A. & Winter, R. (2009). Regulatory compliance in information systems research–literature analysis and research agenda. In *the Proceedings of 14th International Conference of Enterprise, Business-Process and Information Systems Modeling*. Amsterdam, Netherlands.

Corradini, F., Angelis, F., Polzonetti, A., Re, B. & Brugnoni, E. (2006). e-GovQoS: An Ontology for Quality of E-Government Services. In *Proceedings of the 5th International Conference on Electronic Government*. Krakow, Poland.

Corrales, M., Jurčys, P., & Kousiouris, G. (2019). Smart contracts and smart disclosure: coding a GDPR compliance framework. In *Legal Tech, Smart Contracts and Blockchain (189-220)*. Springer, Singapore.

Corrales M. & Kousiouris G. (2017). Nudging Cloud Providers: Improving Cloud Architectures Through Intermediary Services. In Corrales M., Fenwick M., Forgó N. (Ed.), *New Technology, Big Data and the Law* (p.151-186). Springer, Singapore.

Costilla, C., Palacios, J., Cremades, J. & Vila, J. (2005). E-Government: A Legislative Ontology for the 'SIAP' Parliamentary Management System. In Böhlen, M., Gamper, J., Polasek, W, & Wimmer, M. (Ed.). *E-Government: Towards Electronic Democracy* (p.134-146). Springer Berlin Heidelberg.

Culnan, M. J. & Williams, C. C. (2009). How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. *MIS Quarterly, 33*(4), 673-687.

Dada, D. (2006). The Failure of E-Government in Developing Countries: A Literature Review. *The Electronic Journal on Information Systems in Developing Countries, 26*(1), 1 -10.

DeVos, M., Kirrane, S., Padget, J., & Satoh, K. (2019). ODRL policy modelling and compliance checking. In *Proceedings of the 3rd International Conference on Rules and Reasoning*. Bolzano, Italy.

DO LAP HIEN (2017). E-Government Policy of Vietnam. Available at https://www.itu.int/en/ITU-D/RegionalPresence/AsiaPacific/Documents/Events/2017/Sep-SCEG2017/SESSION-2_Vietnam_Mr_Lap_Hien_Do.pdf. Accessed on 14 July 2020.

Dombeu, J. (2010). A conceptual ontology for E-Government monitoring of development projects in Sub Saharan Africa. In *IST-Africa*. Durban, South Africa.

El-Kharbili, M. & Stolarski, P. (2009). Building-Up a Reference Generic Regulation Ontology: A Bottom-Up Approach. In Abramowicz, W. & Flejter, D. (Ed.). *Business Information Systems Workshops* (p.268-279). Springer Berlin Heidelberg.

EUROPA (2019). The European E-Government Action Plan 2016-2020. Available at https://ec.europa.eu/digital-single-market/en/european-egovernment-action-plan-2016-2020. Accessed on 14 July 2020.

EUROPA (2018). *General Data Protection Regulation (GDPR).* Available at https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en#legislation. Accessed on 14 July 2020.

EUROSTAT (2020). *E-Government – more citizens consult information online*. Available at https://ec.europa.eu/eurostat/web/products-eurostat-news/-/EDN-20200307-1. Accessed on 14 July 2020.

European Commission (2019). *Digital Government Factsheet 2019 - Greece*. Available at https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Greece_2019.pdf, Accessed on 14 July 2020.

Falbo, A., Natali, C., Mian, G., Bertollo, G., Ruy, B. (2003). ODE: Ontology-based software development environment. In *Argentine Congress on Computer Science*. La Plata, Argentina.

Färber, M., Bartscherer, F., Menne, C., & Rettinger, A. (2018). Linked data quality of dbpedia, freebase, opencyc, wikidata, and yago. *Semantic Web, 9*(1), 77-129.

Fragkou, P., Galiotou, E., Matsakas, M. (2014). Enriching the e-GIF Ontology for an Improved Application of Linking Data Technologies to Greek Open Government Data. *Procedia-Social and Behavioral Sciences Journal 147*(2014), 167-174.

FTC.Gov (1970). *Fair Credit Reporting Act*. Available at https://www.ftc.gov/enforcement/ statutes/fair-credit-reporting-act. Accessed on 14 July 2020.

FTC.Gov (1999). *The Gramm-Leach-Bliley Act of 1999*. Available at https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act. Accessed on 14 July 2020.

FTC - Federal Trade Commission (2009). *Consumer Data Broker ChoicePoint Failed to Protect Consumers' Personal Data, Left Key Electronic Monitoring Tool Turned Off for Four Months*. Available at https://www.ftc.gov/news-events/press-releases/2009/10/consumer-data-broker-choicepoint-failed-protect-consumers, Accessed on 6 November 2018.

G-Cloud (2020). Government Cloud: A strategic choice for Greek public sector modernization. Available at https://witsa.org/wp-content/uploads/2018/01/2018_G_Cloud_ project-nomination.pdf. Accessed on 14 July 2020.

Gerontas, A. (2020). Towards an e-Government semantic interoperability assessment framework. In *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance,* Athens, Greece.

Gharib, M., Mylopoulos, J. & Giorgini, P. (2020). COPri-A Core Ontology for Privacy Requirements Engineering. In *14th International Conference on Research Challenges in Information Science*, Limassol, Cyprus.

Giblin, C., Müller, S., Pfitzmann, B. (2006). From regulatory policies to event monitoring rules: Towards model-driven compliance automation. *Technical Report, IBM Research Zurich*.

Glover, I., Xu, Z., & Hardaker, G. (2007). Online annotation–Research and practices. *Computers & Education*, *49*(4), 1308-1320.

Goedert, J. (2011). *TRICARE Hit with $4.9 Billion Suit Following Breach.* Available at https://www.healthdatamanagement.com/news/tricare-hit-with-49-billion-suit-following-breach, Accessed on 6 November 2018.

Goldkuhl, G. (2011). Generic regulation model: the evolution of a practical theory for e-government. *Transforming Government: People, Process and Policy*, *5*(3), 249-267.

Gómez-Pérez, A., Ortiz-Rodríguez, F. & Villazón-Terrazas, B. (2006). Legal Ontologies for the Spanish E-Government. In Marín, R., Onaindía, E., Bugarín, A. & Santos, J. (Ed.). *Current Topics in Artificial Intelligence* (p. 301-310). Springer Berlin Heidelberg.

Gómez-Pérez, A. (1995). Some Ideas and Examples to Evaluate Ontologies. In *Proceedings of the 11th Conference on Artificial Intelligence for Applications*. Los Angeles, USA.

Gouscos, D., Mentzas, G. & Georgiadis, P. (2001). Planning and Implementing E-Government Service Delivery: Achievement and Learning from On-line Taxation in Greece. In *Proceedings of the 8th Panhellenic Conference on Informatics*. Nicosia, Cyprus.

Graham, S. & Aurigi, A. (1997). Virtual Cities, Social Polarisation, and the Crisis in Urban Public Space. *Journal of Urban Technology, 4*(1), 19-52

Gronlund, A., & Andersson, A. (2006). E-Government Research Quality Improvements Since 2003: More Rigor, but Research (Perhaps) Redefined. In *Proceedings of the 5th International Conference.* Krakow, Poland.

Gruber, T. R. (1995). Toward Principles for the Design of Ontologies Used for Knowledge Sharing. *International Journal Human Computer Studies, 43*(5/6), 907-928.

Gunda, S. G. (2008). Requirements Engineering: Elicitation Techniques. *University West, Department of Technology, Mathematics and Computer Science*.

Hale, M. & Gamble, R. (2019). Semantic hierarchies for extracting, modeling, and connecting compliance requirements in information security control standards. *Requirements Engineering 24*(3), 365-402.

Hallberg, N., Jungert, E., Pilemalm, S. (2014). Ontology for Systems Development. *International Journal of Software Engineering and Knowledge Engineering 24*(3), 329-34.

Hartley, S. (2018). *Project Management: A practical guide to planning and managing projects*. London, Routledge.

Hartmann, J., Sure, Y., Giboin, A., Maynard, D., del Carmen Surez-Figueroa, M., Cuel, R. (2004). Methods for ontology evaluation. *Technical report, University of Karlsruhe, Germany*.

Hasan, M. M., Anagnostopoulos, D., Kousiouris, G., Stamati, T., Loucopoulos, P., & Nikolaidou, M. (2019). An Ontology based Framework for E-Government Regulatory Requirements Compliance. *International Journal of E-Services and Mobile Applications (IJESMA), 11*(2), 22-42.

Henderson-Sellers, B., Gonzalez-Perez, C., Mcbride, T., & Low, G. (2014). An ontology for ISO software engineering standards: 1) Creating the infrastructure. *Computer Standards & Interfaces, 36*(3), 563-576.

Hevner, A. & Chatterjee, S. (2010). Design science research in information systems. In Hevner, A. and Chatterjee, S. (Ed.). *Design Research in Information Systems: Theory and Practice (Integrated Series in Information Systems)* (p. 9–22). Springer Boston US.

HHS.Gov (1996). *The Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. Available at https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html. Accessed on 14 July 2020.

Horridge, M., Knublauch, H., Rector, A., Stevens, R. & Wroe, C. (2004). A Practical Guide to Building OWL Ontologies Using the Protégé tool. *University of Manchester, United Kingdom (UK).*

Hughes, R. T. (2010). Project management process ontologies: a proof of concept. In *Proceedings of the 15th Conference of UK Academy for Information Systems.* UK.

Hwang, W. Y., Wang, C. Y., & Sharples, M. (2007). A study of multimedia annotation of Web-based materials. *Computers & Education*, *48*(4), 680-699.

Ingolfo, S., Siena, A., & Mylopoulos, J. (2011). *Establishing Regulatory Compliance for Software Requirements*. Conceptual Modeling M. Jeusfeld, L. Delcambre and T.-W. Ling, Springer Berlin Heidelberg, 47-61.

IT Governance (2013). ISO/IEC 27001 - International Security Standard. Available at https://www.itgovernance.co.uk/iso27001. Accessed on 14 July 2020.

Jaeger, P. T. (2008). User-centered policy evaluations of section 508 of the rehabilitation act: Evaluating E-Government web sites for accessibility for persons with disabilities. *Journal of Disability Policy Studies*, *19*(1), 24-33.

Jansson, G. (2012). Contemporary Ideas in the Framing of a European Policy for E-Government. In *Proceedings of the 34th EGPA (European Group of Public Administration) Conference*. Bergen, Norway.

Kalampokis, E., Zeginis, D., & Tarabanis, K. (2019). On modeling linked open statistical data. *Journal of Web Semantics*, *55*(2019), 56-68.

Kalogirou, V., Stasis, A., & Charalabidis, Y. (2020). Adapting national interoperability frameworks beyond EIF 3.0: the case of Greece. In *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance*. Athens, Greece.

Karyda, M., Balopoulos, T., Dritsas, S. Gymnopoulos, L., Kokolakis, S., Lambrinoudakis, C. & Gritzalis, S. (2006). An ontology for secure E-Government applications. In *Proceedings of the 1st International Conference on Availability, Reliability and Security*. Vienna, Austria.

Kendall, E. F. & McGuinness, D. L. (2019). Ontology engineering. *Synthesis Lectures on The Semantic Web: Theory and Technology 9*(1), 1-102.

Khan, R.A., Li, T. and Khan, A. (2019). Cloud Migration: Standards and Regulatory Issues with Their Possible Solutions. *International Journal of Advanced Networking and Applications*, *10*(6), 4113-4119.

Kitchenham, B., Pretorius, R., Budgen, D., Pearl Brereton, O., Turner, M., Niazi, M. & Linkman, S. (2010). Systematic literature reviews in software engineering – A tertiary study. *Information and Software Technology*, *52*(8), 792-805.

Kitchenham, B. A., Travassos, G. H., VonMayrhauser, A., Niessink, F., Schneidewind, N. F., Singer, J., Takada, S., Vehvilainen, R., Yang, H. (1999). Towards an ontology of software maintenance. *Journal of Software Maintenance: Research and Practice 11*(6), 365-389.

Khadraoui, A., Arni-Block, N., Léonard, M. & Ralyté, J. (2008). Laws-Based Ontology for E-Government Services Construction Case Study: The Specification of Services in Relationship with the Venture Creation in Switzerland. In Stirna, J. & Persson, A. (Ed.). *The Practice of Enterprise Modeling* (p.197-209). Springer Berlin Heidelberg.

Khadraoui, A., Arni-Block, N., Léonard, M. & Ralyté, J. (2005). Laws-based ontology for e-Government information systems. In *Proceedings of the 2nd International conference on innovations in information technology IIT*. Dubai, UAE.

Kleine, D. (2009). The ideology behind the technology – Chilean microentrepreneurs and public ICT policies. *Geoforum 40*(2), 171-183.

Kousiouris, G., Vafiadis, G., & Corrales M. (2013). A Cloud provider description schema for meeting legal requirements in cloud federation scenarios. In *Proceedings of the 12th Conference on e-Business, e-Services and e-Society*. Athens, Greece.

Kromidha, E. (2012). Strategic E-Government development and the role of benchmarking. *Government Information Quarterly, 29*(4), 573-581.

Kumar, R. (2018). *Research methodology: A step-by-step guide for beginners*. Sage Publication.

Kuzma, J. M. (2010). Accessibility design issues with UK E-Government sites. *Government Information Quarterly, 27*(2), 141-146.

Kvasnicova, T., Kremenova, I., & Fabus, J. (2016). From an analysis of e-services definitions and classifications to the proposal of new e-service classification. *Procedia Economics and Finance 100*(39), 192-196.

Layne, K. & Lee, J. (2001). Developing fully functional E-Government: A four stage model. *Government information quarterly, 18*(2), 122-136.

Law Insider (2020). *Definition of Regulatory Requirements*. Available at https://www.lawinsider.com/dictionary/regulatory-requirements. Accessed on 14 July 2020.

Lemey, E. & Poels, G. (2011). Towards a service system ontology for service science. In *the Proceedings of the 9th International Conference on Service-Oriented Computing*. Paphos, Cyprus.

Leppanen, M. (2006). Towards an ontology for information systems development. In *Proceedings of the 18th Conference on Advanced Information Systems Engineering*. Luxembourg.

Lofstedt, U. (2012). E-Government - assessment of current research and some proposals for future direction. *International Journal of Public Information System*, *1*(1).

Magoutas, B., Halaris, C., & Mentzas, G. (2007). An Ontology for the Multi-Perspective Evaluation of Quality in E-Government Services. In M. Wimmer, Scholl, J. & Grönlund, Å. (Ed.). *Electronic Government* (p. 318-329). Springer Berlin Heidelberg.

Markusheuski, D., Rabava, N., & Kukharchyk, V. (2017). Blockchain technology for e-governance. In *Proceedings of the Conference of Innovation Governance in the Public Sector*. Atlanta, Georgia, USA.

Massey, A. K., Rutledge, R. L., Antón, A. I., & Swire, P. P. (2014). Identifying and classifying ambiguity for regulatory requirements. In *Proceedings of the 22nd international requirements engineering conference*. Karlskrona, Sweden.

Massey, A. K., Otto, P. N., & Anton, A. I (2009). Prioritizing Legal Requirements. In *Proceedings of the 2nd International Workshop on Requirements Engineering and Law*. Atlanta, Georgia, USA.

Maxwell, J. C., Antón, A. I., Swire, P. Riaz, M., & McCraw, C. M. (2012). A legal cross references taxonomy for reasoning about compliance requirements. *Requirements Engineering Journal*, *17*(2), 99-115.

Maxwell, J. C. & Anton, A. I. (2010). The production rule framework: developing a canonical set of software requirements for compliance with law. In *Proceedings of the 1st ACM International Health Informatics Symposium*. Arlington, Virginia, USA.

Mazzola, L. Kapahnke, P., Vujic, M., & Klusch, M. (2016). CDM-Core: A Manufacturing Domain Ontology in OWL2 for Production and Maintenance. In *Proceedings of the 8th International Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*. Portugal.

Middleton, M. (2007). Approaches to evaluation of websites for public sector services. In *Proceedings of the IADIS Conference on e-Society*. Lisbon, Portugal.

Mills, E. (2009). *Choice Point to pay $275,000 in latest data breach*. Available at https://www.cnet.com/news/choicepoint-to-pay-275000-in-latest-data-breach, Accessed on 6 November 2018.

Milton, S. K., Rajapakse, J., & Weber, R. (2012). Ontological clarity, cognitive engagement, and conceptual model quality evaluation: An experimental investigation. *Journal of the Association for Information Systems 13*(9), 657.

Ministry of Finance – Singapore (2015). *EGov2015 Masterplan (2011-2015): Connecting People, Enriching Lives*. Available at https://www.mof.gov.sg/policies/e-government. Accessed on 14 July 2020.

Mishra, S. & Alok, S. (2011). *Handbook of Research Methodology*. Educreation Publishing, New Delhi.

Mockus, M., & Palmirani, M. (2017). Legal ontology for open government data mashups. In *Proceedings of the IEEE Conference for E-Democracy and Open Government*. Krems, Austria.

Mustapha, A., Arogundade, O., Misra, S., Damasevicius, R., & Maskeliunas, R. (2020). A systematic literature review on compliance requirements management of business processes. *International Journal of System Assurance Engineering and Management, 11*(3), 561-576.

Muthuri, R., Boella, G., Hulstijn, J., Capecchi, S., & Humphreys, L. (2017). Compliance patterns: harnessing value modeling and legal interpretation to manage regulatory conversations. In *Proceedings of the 16th International Conference on Artificial Intelligence and Law*. London, United Kingdom.

Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2019). Information privacy practices in e-government in an African least developing country, Rwanda. *The Electronic Journal of Information Systems in Developing Countries*, *85*(2), 12074.

Nakakawa, A., & Namagembe, F. (2019). Requirements for developing interoperable e-government systems in developing countries-a case of Uganda. *Electronic Government, an International Journal*, *15*(1), 67-90.

Nanos, I., Misirlis, N., & Manthou, V. (2017). Cloud Computing Adoption and E-government. In *Proceedings of the 28th National Conference on Operational Research*. Thessaloniki, Greece.

Niculescu, C., & Trausan-Matu, S. (2009). An ontology-centered approach for designing an interactive competence management system for IT companies. *Informatica Economica*, *13*(4), 159 – 167.

Noy, N. F. & McGuinness, D. L. (2001). Ontology Development 101: A Guide to Creating Your First Ontology. *Stanford University, USA.*

Nyren, O., Stenbeck, M., & Gronberg, H. (2014). The European Parliament proposal for the new EU General Data Protection Regulation may severely restrict European epidemiological research. *European Journal of Epidemiology, 29*(4), 227-230.

OECD (2020). *E-Government for Better Government.* Available at https://www.oecd.org/ gov/digital-government/e-governmentforbettergovernment. htm. Accessed on 14 July 2020.

Okike, E. U. (2017). SQS: An Ontology Based Framework for Evaluating Service Oriented Software Applications: A case study of E-Governance *Services. The International Journal of Computer Science and Information Security (IJCSIS), 15*(12), 1-6.

Olbrich, S. & Simon, C. (2008). Process Modelling towards E-Government-Visualisation and Semantic Modelling of Legal Regulations as Executable Process Sets. *Electronic Journal of E-Government*, *6*(1), 43-54.

Olson, D. (2020). *Core Concepts of Project Management*. Business Expert Press.

Olszewska, J. I. & Allison, I. K. (2018). ODYSSEY: Software Development Life Cycle Ontology. In *Proceedings of the 10th International Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*. Seville, Spain.

Ortiz-Rodríguez, F. & Villazón-Terrazas, B. (2006). EGO Ontology Model: law and regulation approach for E-Government. In *Proceedings of the 3rd Conference on European Semantic Web*. Budva, Montenegro.

Othman, M. H., & Razali, R. (2017). Electronic government systems interoperability model. *Journal of Telecommunication, Electronic and Computer Engineering*, *9*(3-4), 1-9.

Oveh, R. & Egbokhare, F. (2020). Software Process Ontology Evaluation Using Ontoclean. *Journal of Science and Technology Research 2*(1), 55-61.

Pak, J., & Zhou, L. (2009). A framework for ontology evaluation. In *Proceedings of the 8th International Workshop on Exploring the Grand Challenges for Next Generation E-Business*. Phoenix, USA.

Peffers, K., Tuunanen, T., Rothenberger, M.A., and Chatterjee, S., (2007). A Design Science Research Methodology for Information Systems Research. *Journal of management information systems, 24*(3), 45-77.

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2006). The design science research process: a model for producing and presenting information. In *Proceedings of the 1st international conference on design science research in information systems and technology*. Worcester, MA, USA.

Petersen, K., Feldt, R., Mujtaba, S. & Mattsson, M. (2008). Systematic mapping studies in software engineering. In *Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering*. Swindon, UK.

Piccinelli, G., & Stammers, E. (2002). From e-processes to e-networks: an e-service-oriented approach. In *Proceedings of the 3rd International Conference on Internet Computing*. Las Vegas, Nevada, USA.

Polleres, A., Kamdar, M. R., Fernández, J. D., Tudorache, T., & Musen, M. A. (2020). A more decentralized vision for linked data. *Semantic Web, 11*(1), 101-113.

Pressman, R. S. (2014). *Software engineering: A practitioner's approach*. 8th Edition. New York: McGraw-Hill.

Prins, C. (2007). E-Government: A Comparative Study of the Multiple Dimensions of Required Regulatory Change. *Electronic Journal of Comparative Law, 11*(3), 1-23.

Public Service Management and Good Governance (2017). *E-Government Guidelines*. Available at https://www.ega.go.tz/uploads/standards/sw-1574918368-level1%20big.pdf. Accessed on 14 July 2020.

Rahmadika, S. & Rhee, K. H. (2018). Blockchain technology for providing an architecture model of decentralized personal health information. *International Journal of Engineering Business Management, 10*(2018), 1-12.

Rehman, K., Shah, A. A., & Ahmed, K. (2018). E-Government Identification to Accomplish Sustainable Development Goals (UN 2030 Agenda) A Case Study of Pakistan. In *Proceedings of the IEEE Global Humanitarian Technology Conference*. California, USA.

Rocha, R., Araujo, A., Cordeiro, D., Ximenes, A., Teixeira, J., Silva, G., & Duarte, M. (2018). DKDOnto: An Ontology to Support Software Development with Distributed Teams. *Procedia Computer Science*, *126*(2018), 373-382.

Ruhode, E. (2016). E-Government for Development: A Thematic Analysis of Zimbabwe's Information and Communication Technology Policy Documents. *The Electronic Journal of Information Systems in Developing Countries*, *73*(1), 1-15.

Ruiz, F., Vizcaíno, A., Piattini, M., García, F. (2004). An ontology for the management of software maintenance projects. *International Journal of Software Engineering and Knowledge Engineering 14*(3), 323-349.

Sack, K. (2011). *Patient Data Landed Online After a Series of Missteps.* The New York Times, Available at https://www.nytimes.com/2011/10/06/us/stanford-hospital-patient-data-breach-is-detailed.html, Accessed on 6 November 2018.

Sadiq, S., Governatori, G. & Naimiri, K. (2007). Modeling Control Objectives for Business Process Compliance. In *Proceedings of the 5th International Conference on Business Process Management*. Brisbane, Australia.

Saidane, A. and Al-Sharieh, S. (2019). A Compliance-Driven Framework for Privacy and Security in Highly Regulated Socio-Technical Environments: An E-Government Case Study. In Abassi, R. and Douss (Ed.), *Security Frameworks in Contemporary Electronic Government (pp.15-50),* IGI Global Publisher.

Salhofer, P., Stadlhofer, B., & Tretter, G. (2009). Ontology driven E-Government. In *Proceedigns of the 4th International Conference on Software Engineering Advances*. Porto, Portugal.

Sarantis, D. & Askounis, D. (2009). A project management ontology as a reference for E-Government projects. In *Proceedings of the 4th International Conference on Internet Technology and Secured Transactions*. London, UK.

Schmidt, R., Bartsch, C., & Oberhauser, R. (2007). Ontology-based Representation of Compliance Requirements for Service Processes. In *Workshop on Semantic Business Process and Product Lifecycle Management.* Innsbruck, Austria.

Scupola, A., Henten, A., & Nicolajsen, H. W. (2009). E-Services: Characteristics, Scope and Conceptual Strengths. *International Journal of E-Services and Mobile Applications*, *1*(3), 1–16.

Sheeba, T., Krishnan, R., & Bernard, M. J. (2012). An ontology in project management knowledge domain. *International Journal of Computer Applications 56*(5), 1-7.

Shehu, J. & Xhina, E. (2019). Modeling an ontology for public E-Government Services in Albania. In *Proceedings of the International Academic Conference on Research in Engineering and Technology*. Barcelona, Spain.

Siena, A., Armellin, G., Mameli, G., Mylopoulos, J., Perini, A., & Susi, A. (2010). Establishing regulatory compliance for information system requirements: An experience report from the health care domain. In *Proceedings of the 29th International Conference on Conceptual Modeling*. Vancouver, Canada.

Soliman, J., Formoso, T., & Tzortzopoulos, P. (2020). A semantic-based framework for automated rule checking in healthcare construction projects. *Canadian Journal of Civil Engineering*, *47*(2), 202-214.

SOX Law (2002). *The Sarbanes-Oxley Act of 2002*. Available at http://www.soxlaw.com. Accessed on 14 July 2020.

Stojanovic, L., Abecker, A., Stojanovic, N., & Studer, R. (2004). On managing changes in the ontology-based E-Government. In *Proceedings of the International Conferences on the Move to Meaningful Internet Systems*. Agia Napa, Cyprus.

Stratigaki, C., Nikolaidou, M., Loucopoulos, P., & Anagnostopoulos, D. (2016). Business Process Elicitation from Regulatory Compliance Documents: An E-Government Case Study. In *Proceedigns of the 18th Conference on Business Informatics*. Paris, France

Stumpe, F. (2018). Ontology in IT Projects Based on OSM. *Ontology in Information Science*, InTech, 129.

Sulistiyani, E. & Susanto, T. D. (2018). Change Management Methodology for e-Government Project in Developing Countries: A Conceptual Model. In *Proceedings of the 3rd International Conference on Informatics and Computing*. Palembang, Indonesia.

Syed, R. (2019). Enterprise reputation threats on social media: A case of data breach framing. *The Journal of Strategic Information Systems*, *28*(3), 257-274.

Tebes, G., Olsina, L., Peppino, D., & Becker, P. (2020). TestTDO: A Top-Domain Software Testing Ontology. In *23rd Iberoamerican Conference on Software Engineering*, Curitiba, Brazil.

Thomas, M. A. & Elnagar, S. (2018). A Semantic Approach to Evaluate Web Content of Government Websites. *Innovative Perspectives on Public Administration in the Digital Age*, *1*(1), 1-24.

UN Report (2020). *United Nations E-Government Survey 2020*. Available at https://www.un.org/development/desa/publications/publication/2020-united-nations-e-government-survey Accessed on 14 July 2020.

Van Ruijven, L. C. (2013). Ontology for systems engineering. *Procedia Computer Science*, *16*, 383-392.

Vassilakis, C. & Lepouras, G. (2006). Ontology for E-Government public services. *Encyclopedia of E-Commerce, E-Government, and Mobile Commerce*, p. 865-870. IGI Global.

Vijayan (2011). *Difense Dept. hit with $4.9 B lawsuit over data breach*. Available at https://www.computerworld.com/article/2499000/data-privacy/defense-dept--hit-with--4-9b-lawsuit-over-data-breach.html, Accessed on 6 November 2008.

Voss, W (2014). Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later. *Journal of Internet Law, 17*(9), 1-15.

Wand, Y., Storey, V., & Weber, R. (1999). An ontological analysis of the relationship constructs in conceptual modeling. *ACM Transactions on Database Systems 24*(4), 494-528.

Wang, X., Yu, G., & Peng, Y. (2020). Research on Dynamic Business Process Modeling of E-Government System Based on Extended ECA Rules. In *Proceedings of the 3rd International Conference on Social Science, Public Health and Education*. Xiamen, China.

Wibowo, A. & Davis, J. (2020). Requirements Traceability Ontology to Support Requirements Management. In *Proceeding of the Australasian Computer Science Week Multiconference*, Melbourne, Australia.

Wiegers, K. & Beatty, J. (2013). *Software requirements*. Pearson Education.

Webster, J. & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a Literature Review. *MIS Quarterly, 26*(2), 13-23.

Wimmer, M., Codagnone, C., & Janssen, M. (2008). Future of E-Government Research: 13 research themes identified in the eGovRTD2020 project. In *Proceedings of the 41st Hawaii International Conference on System Sciences.* USA.

Wongthongtham, P., Kasisopha, N., Chang, E., & Dillon, T. (2008). A software engineering ontology as software engineering knowledge representation. In *Proceedings of the 3rd International Conference on Convergence and Hybrid Information Technology*. Busan, South Korea.

Xiao, Y., Xiao, M., & Zhao, H. (2007). An ontology for E-Government knowledge modeling and interoperability. In *Proceedings of the 3rd International Conference on Wireless Communications, Networking and Mobile Computing.* Shanghai, China.

Xiong, J (2006). Current status and needs of Chinese E-Government users. *Emerald Electronic Library, 24*(6), 747-762.

Xu X. & Cai H. (2019). Semantic Frame-Based Information Extraction from Utility Regulatory Documents to Support Compliance Checking. In Mutis I. & Hartmann T. (eds). *Advances in Informatics and Computing in Civil and Construction Engineering* (pp 223-230). Springer, Cham.

Yang, L., Cormican, K., & Yu, M. (2019). Ontology-based systems engineering: A state-of-the-art review. *Computers in Industry*, 111: 148-171.

Yanuarifiani, A. P., Chua, F. F., & Chan, G. Y. (2020). An Ontology Framework for Generating Requirements Specification. *International Journal on Advanced Science, Engineering and Information Technology, 10*(3), 1137.

Yao, Z., Peddamail, J. R., & Sun, H. (2019). Coacor: Code annotation for code retrieval with reinforcement learning. In The World Wide Web Conference. San Francisco, CA, USA.

Yoon, D. (2018). The policy research of preliminary feasibility study for the government R&D innovation strategy. *International Journal of Engineering Business Management, 10*(2018), 1-11.

Yustianto, P., Doss, R., & Kurniawan, N. B. (2018). Consolidating Service Engineering Ontologies: Building Service Ontology from SOA Modeling Language (SoaML). In *Proceedings of the International Conference on Information Technology Systems and Innovation*. Padang, Indonesia.

Zarrabi, J. F. & Tawil, A. (2019). A High-Level Scheme for an Ontology-Based Compliance Framework in Software Development. In *Proceedings of the 17th International Conference on High Performance Computing and Communications*. New York, USA.

Zarzour, H. & Sellami, M. (2017). A linked data-based collaborative annotation system for increasing learning achievements. *Educational Technology Research and Development 65*(2), 381-397.

Zhang, J. & El-Gohary, N. M. (2016). Semantic NLP-based information extraction from construction regulatory documents for automated compliance checking. *Journal of Computing in Civil Engineering 30*(2), 04015014.

Zulhuda, S. (2012). The state of E-Government security in Malaysia: reassessing the legal and regulatory framework on the threat of information theft. In *Proceedings of the International Conference on Computing and Information Technology*. Madinah, Saudi Arabia.

Appendix A: Ontology Instantiation

GDPR Regulations Text	Derived Individual in the Defined Class
Rule 78: *Controller should adopt internal policies and implement measures which meet in particular the principles of data protection… in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.*	Controller Policy *isA* Internal Regulation; Data Controller *isA* Service Provider
Rule 4(20): *Personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers…of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;*	Data Protection Policy *isA* Internal Regulation; Personal Data Protection *isA* Regulatory Impact
Ruel 32: *Consent should be given by the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including electronic means, or an oral statement.*	Data Subject Agreement *isA* Internal Regulation
Rule 81: *The processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature, and purposes of the processing,*	Data Processor Agreement *isA* Internal Regulation
Rule 4(6): *The data protection officer may be a staff member of the controller/processor or fulfil tasks on the basis of a service contract.*	Service Agreement *isA* Internal Reg.
Rule 42(7): *Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies…by the competent supervisory authority where the requirements for the certification are not or are no longer met.*	Data Controller Agreement *isA* Internal Regulation; Supervisory Authority *isA* Service Provider
Rule 16: *The regulation does not apply to issues of protection of fundamental rights and freedoms, or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security.*	Union Law *isA* External Regulation; European Union *isA* E-Gov Donor

Rule 8: *The regulation provides for specifications or restrictions of rules by the Member State law……necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this regulation into their national law.*	Member State Law *isA* External Regulation
Rule 43(9): *The commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognize those certification mechanisms, seals, and marks and adopted in accordance with examination procedure referred…*	Technical Law *isA* External Regulation; Data Protection Seal *isA* Hardware Resource
Rule 104:*…assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law…norms and standards including legislation regarding public health…*	HIPPA *isA* External Regulation
Rule 81: *To ensure compliance with the…Regulation in respect of the processing…the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organizational measures which will meet the requirements of this Regulation, including for the security of processing.*	Citizen Trust *isA* Regulatory Impact
Rule 2: *The Regulation is intended to contribute to the accomplishment of an area of freedom, security, and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of the natural persons.*	Economic and Social Union *isA* Regulatory Impact
Rule 3: *Directive 95/46/EC of the European Parliament and of the Council seeks to harmonize the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to guarantee the free flow of personal data between Member States.*	Free flow of personal data *isA* Regulatory Impact
Rule 39: *Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted,….and to what extent the personal data are or will be processed.*	Transparency in Data Processing *isA* Regulatory Impact

Rule 157: *By coupling information from registries, researchers can obtain new knowledge with regard to widespread medical conditions such as cardiovascular disease, cancer, and depression…which can provide the basis for formulation and implementation of knowledge… and improve the efficiency of social services.*	Efficient Data processing *isA* Regulatory Outcome
Rule 70: *personal data are processed for the purposes of direct marketing; the data subject should have the right to object to such processing related to such direct marketing.*	Direct Marketing *isA* G2B Service
Rule 89(1): *Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject.*	Historical Research; Scientific Research; Statistical Analysis *isA* G2G Service
Rule 24: *…personal data processing consists of profiling a natural person to take decisions concerning his or her personal preferences, behaviors, and attitudes.*	Profiling Natural Person *isA* G2B Service
Rule 19: *The protection of natural persons with regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and prevention of threats to public security..*	Criminal Investigation *isA* G2G Service; Public Organization *isA* E-Gov User
Rule 39(1b):*…data protection provisions to the protection of personal data, including the assignment of responsibilities, awareness-raising and staff training involved in processing operations and related audits.*	Staff Training *isA* Development Requirement
Rule 82: *In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.*	Testing and Monitoring; Controller-Processor Collaboration *isA* Development Requirement
Rule 39: *The specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.*	Data Collection; Data Processing *isA* E-Gov Service
Rule 63: *A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable*	Data Access *isA* E-Gov Service; *isA* Obligation; Data

intervals, in order to be aware of, and verify, the lawfulness of the processing. It includes the right for data subjects to have access data concerning their health…	Subject *isA* E-Gov User
Rule 14(2a): *the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.*	Data Storing *isA* E-Gov Service
Rule 6: *…free flow of personal data within the Union and the transfer to third countries and international organizations, while ensuring a high level of the protection of personal data*	Data Sharing *isA* E-Gov Service
Rule 7(3): *The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.*	Withdraw Consent *isA* E-Gov Service; *isA* Obligation
Rule 32: *Consent should be given by a clear affirmative act…specific, informed, and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.*	Give Consent *isA* E-Gov Service; Give Consent *isA* Obligation
Rule 141: *Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence,*	Lodge Complain *isA* E-Gov Service
Rule 16(1): *The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.*	Info Rectification *isA* E-Gov Service; *isA* Obligation
Rule 25(2): *…obligation applies to the amount of personal data…the period of their storage and their accessibility… by default personal data are not made accessible without the individual's intervention to an indefinite number of the natural persons*	Data Accessibility *isA* Quality Requirement
Rule 18(1a): *the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;*	Data Accuracy *isA* Quality Requirement
Rule 32(1c): *…restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*	Data Availability *isA* Quality Requirement
Rule 39: *…Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorized access to or use of personal data and the equipment used for the processing.*	Data Security; Confidentiality *isA* Quality Requirement

Rule 68: *The data controllers should be encouraged to develop interoperable formats that enable data portability.*	Data Portability *isA* Quality Requirement
Rule 32(1b): *the controller and processor shall implement appropriate technical and organizational measures to ensure confidentiality, integrity, availability and resilience of processing systems and services.*	Data Resilience *isA* Quality Requirement
Rule 32(1c): *the controller and processor shall implement appropriate technical and organizational measures to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.*	Timeliness *isA* Quality Requirement; Data Processor *isA* Service Provider
Rule 20(1): *The data subject shall have the right to receive personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller*	Transfer only Machine-Readable Data to Controller *isA* Action Rule
Rule 13: *To take account of the specific situation of small and medium-sized enterprises, Regulation includes a derogation for organizations with fewer than 250 employees with regard to record-keeping…*	Maintain Data Processing Record *isA* Action Rule
Rule 12(1): *When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.*	Process Data on Valid Request *isA* Action Rule
Rule 59: *The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.*	Provide Data within One Month *isA* Constraint Rule
Rule 85: *the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it,…*	Report Data breach withing 72 hours *isA* Constraint Rule
Rule 83(4): *Infringements of the following provisions shall be subject to administrative fines up to* 10M€*, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.*	10M€ Penalty for Regulation non-compliance *isA* Computation Rule
Rule 4(1): *'personal data' means any information relating to an identified or identifiable natural person ('data subject');… such as a name, an identification number, location data, an online identifier…*	Personal Data Identification *isA* Fact Rule

Rule 4(14): *biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as the facial images or dactyloscopy data.*	Data Subject Identification *isA* Fact Rule; Biometric Device *isA* Hardware Resource
Rule 9(1): *Processing biometric data for the purpose of uniquely identifying a natural person, data concerning health or natural person's sex life, or sexual orientation shall be prohibited.*	Biometric Data *isA* Private Data
Rule 47(3): *The Commission may specify the format and procedures for the exchange of information between controllers, processors, and supervisory authorities…*	Specify information exchange format *isA* Privilege
Rule 15(3): *The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs.*	Charge Data Processing Fee *isA* Privilege; *isA* Dynamic Rule
Rule 141: *In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.*	Data Subject can Submit Complain Electronically *isA* Privilege
Rule 32(1c): *The ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident.*	Timely Restore Access *isA* Privilege
Rule 47: *The processing of the personal data strictly……constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.*	Business Organization *isA* E-Gov User
Rule 39(1a): *The data protection officer shall inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation.*	Data Protection Officer *isA* Service Provider
Rule 23(1e):*…an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health, and social security.*	National Government *isA* E-Gov Donor

Rule 4(4): *…automated processing of personal data…to analyze or predict aspects concerning natural person's performance at work, economic situation, health, preferences, interests, reliability, behavior, location, or movements.*	Personal Data *isA* Private Data
Rule 83: *In order to maintain data security, the processor should evaluate the risks inherent in the data processing and implement measures to mitigate those risks, such as data encryption techniques.*	Encryption Technique isA Software Resource