How TOGAF® can address government interoperability problems
A case study of the government of Canada

Yuxun Ji
University of Melbourne
yuxunj@student.unimelb.edu.au

Pai Zhang
University of Melbourne
paizhang@student.unimelb.edu.au

Changsheng Qiu
University of Melbourne
changshengq@student.unimelb.edu.au

Peiyao Li
University of Melbourne
peiyaol1@student.unimelb.edu.au

Dexian Wang
University of Melbourne
dexianw@student.unimelb.edu.au

Abstract

Governments are paying more and more attention to the development of digital transformation. Governments have found that systems across departments are not always compatible, leading to interoperability problems. Solving these interoperability problems to provide higher quality services to citizens has become the primary problem that governments must address. Therefore, we raise the following research question: How can TOGAF® assist in addressing government interoperability problems? By analysing the advantages and disadvantages of four enterprise architectures, we find that TOGAF® is the most suitable framework to solve interoperability problems for governments. The article also cites the successful interoperability solution of the Canadian government to demonstrate this paper's arguments.

Acknowledgement

Many thanks to our research supervisor Dr Rod Dilnutt, Industry Fellow, The University of Melbourne.

1. Introduction

In the digital era, governments are seeking online opportunities to enhance efficiency and increase the well-being for citizens and communities. Governments choose different infrastructure and solutions to meet their online service delivery needs. However, public services may require various entities to exchange information, while the ICT solutions of different departments are not always compatible with each other. This immaturity of interoperability leads to inefficiency and waste of resources (Jiménez et al., 2014). Hence, the issue of interoperability is regarded as one of the biggest challenges for the delivery of e-government services. An appropriate enterprise architecture framework (EAF) is required in building government interoperability robustness.

This paper aims to explore the question "How can TOGAF® assist in addressing government interoperability problems?" It will firstly discuss the current state of e-government and its interoperability issues. Four architecture frameworks will be explored: Zachman Framework™, TOGAF®, FEAF, and DoDAF. The TOGAF® framework, regarded as suitable for government interoperability, will be recommended and supported by a case study from the Canadian government.

1.1. Current state of e-government

The capabilities of e-government are changing from the digitalisation of paper-based services to speedy administration services with economic improvement, transparency, and encouragement of participation in government affairs (Sulehat & Taib, 2016). The complexity of information flow requires the government to collaborate as an integrated whole with the public (Goldkuhl, 2008). However, interoperability is regarded as one of the most significant issues in e-government, as it is hard to exchange information between departments. This may result from using different ICT solutions and infrastructures without standardisation and integrated enterprise architecture (EA). Consequently, citizens must continue to visit different government offices and little benefit from digitalisation is shown.

Interoperability is greatly emphasized in countries that have established a mature e-government EA. For instance, interoperability is required in 9 out of 10 standards published by the US National Institute of Standards and related agencies (Jiménez et al., 2014). Additionally, a survey from UNDP (Lallana, 2007) suggests that among the six principles of EAF, interoperability and openness are the only two principles that are emphasised by all countries being investigated (see Figure 1). Hence, a government interoperability framework is required.

	Interoperability	Scalability	Reusability	Openness	Market Support	Security
Australia	●	●	●	●	●	●
Brazil	●	●		●	●	
Denmark	●	●	●	●		●
EU	●		●	●		●
Germany	●	●	●	●		
Malaysia	●			●	●	
UK	●	●		●	●	

Figure 1 - Comparative principles of selected GIFs in 7 countries (Lallana, 2007).

2. Literature Review

2.1. Interoperability

Interoperability in government refers to the ability of different portals or systems to easily communicate with each other and share information. According to previous scholars' research on government interoperability capabilities, it is mainly divided into three levels: Technical Interoperability, Semantic Interoperability and Organisational Interoperability (Novakouski & Lewis, 2012). Technical interoperability is used to describe the technical ability of different programs to exchange data through a common set of interchange formats, to read and write the same file formats, and to use the same protocols. Semantic interoperability allows stakeholders to describe requirements without considering technical implementation. Organisational Interoperability involves how different organisations collaborate to achieve their mutually agreed electronic government goals (Gottschalk, 2009). Organisations need to

reach detailed agreements on the collaboration and synchronisation of their business processes to provide integrated government services. Interoperability helps to promote the efficient collaboration of government systems, the innovation and transformation of government architecture and the delivery of seamless government services. How to use the above capabilities to help the government promote the construction of its architecture plays a key role (Pardo et al., 2012).

2.2. Interoperability challenges

Building high-quality government architecture continues to be recognised as a key strategy for improving government services and the effectiveness of public policies and programs (Oliveira & Eler, 2017), where interoperability is a key factor in testing the maturity level of government architecture (Janssen et al., 2011). Interoperability can be a challenge precisely because government systems need to establish connections with various departments, public and private organisations, exchange of data, language barriers, different format specifications, and varying taxonomies. In addition, the interoperability of e-government systems also has interrelated legal, political and socio-cultural aspects. Government systems also fail because of the technical complexity involved in systems with small linkages to relevant stakeholders, the siloed and fragmented nature of the systems leads to heterogeneity, and the lack of insight into dependencies between organisational and technological aspects hinders progress (Janssen et al., 2011).

2.3. Enterprise Architecture

EA is the collection of architectural and strategic disciplines of an organisation that consists of the business processes and information systems, and their interrelationships (Perks & Beveridge, 2003). An EA framework is an adaptable, scalable, and conceptual foundation for an enterprise's architecture representation (Perks & Beveridge, 2003). EA can lead to organisational benefits through Resource Complementarity, Organisational Alignment, Information Availability, and Resource Portfolio (Tamm et al., 2011). The application of EA can be seen across a wide range of industries. The government sector is also among the top three industries that are bonded with the EA community compared to the other industries (Carr & Else, 2018). Many professional organisations and governmental institutions have developed their EAFs. The following sub-sections will discuss these four frameworks: ZFEA™, TOGAF®, FEAF, and DoDAF.

2.3.1. Zachman Framework for Enterprise Architecture (ZFEA)™

John A. Zachman proposed ZFEA™ in the late 1980s, and it presents a holistic, descriptive view of EA, providing understanding and insights into the organisation (Gerber et al., 2020). The framework is made up of a bounded 6 x 6 matrix-like structure with columns representing Communication Interrogatives and rows representing Reification Transformation (Zachman, 2009). The intersections between the columns and rows created 36 cells covering every aspect of an enterprise.

However, ZFEA™ can be challenging in actual cases, because its large number of cells and the relationships between cells are not well defined (Sitton & Reich, 2015). ZFEA™ does not provide any process definition for building an EA (Mohamed et al., 2012) or direction for implementation (Sitton & Reich, 2015). It is only a classification scheme for the descriptive representation of complex objects (Sitton & Reich, 2015). In addition, the framework is less responsive to change because it is a static framework, especially in the aspects of technology (Herdiana, 2018).

2.3.2. The Open Group Architecture Framework (TOGAF®)

The TOGAF® standard is an open framework for EA developed by The Open Group, and it is one of the most popular frameworks in most industries (Carr & Else, 2018). TOGAF® is divided into several independent parts, including Architecture Development Method, ADM Guidelines & Techniques, Architecture Content Framework, Enterprise Continuum & Tools, and Architecture Capability Framework (The Open Group, 2018). These parts can be used as a whole or only selecting some of them for adoption (The Open Group, 2018). The TOGAF® ADM is the core of the TOGAF® standard which presents an iterative EA development process, and its cycle is represented in Figure 2 (The Open Group, 2018). Through the ADM cycle, requirements management would occur in all phases, and the results need to be frequently validated against the original expectations (The Open Group, 2018).

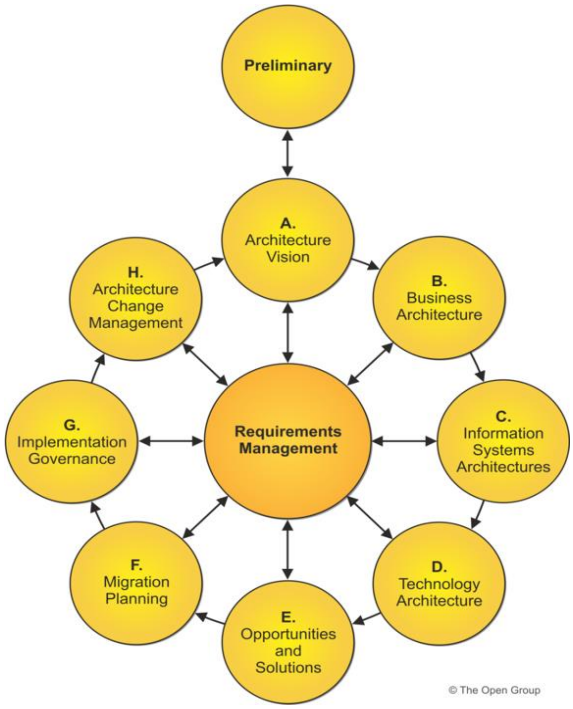

Figure 2. TOGAF® Architecture Development Cycle (The Open Group, 2018)

2.3.3. Department of Defense Architecture Framework (DoDAF)

DoDAF is the comprehensive and conceptual framework that helps Department of Defense (DoD) managers at all levels make effective decisions. There are three groups of views used to explain the DoDAF: the operational views, the systems views, and the technical views. These views serve as the foundation for developing metrics such as performance or interoperability and assessing the influence of the metrics' values on task effectiveness and operational mission (Xuemin et al., 2012).

The DoDAF establishes guidelines and principles for building, representing, and comprehending architectures with a common denominator that spans DoD, joint, and international boundaries (U.S. DoD Architecture Framework Working Group, 2010). The DoDAF guarantees that architecture descriptions can be compared and connected across projects, mission areas, and, eventually, the enterprise, laying the groundwork for studies that support DoD decision-making processes (Xuemin et al., 2012). However, DoDAF was explicitly developed for the U.S. Department of Defense to support their combat operations and no longer used by the E-Government program (Mohamed et al., 2012).

2.3.4. Federal Enterprise Architecture Framework (FEAF)

FEAF is a framework proposed by the Chief Information Officers Council (CIO Council) (Ji & Xia, 2007). The FEAF consists of four levels. The highest level of the architecture framework, level 1 is mainly concerned with the strategic direction of various architecture drivers and architecture. Level 2 provides a more detailed analysis of the drivers, identifying the target business architecture and design architecture. Level 3 takes the business, data, application, and technology of several viewpoints as the target architecture to establish the model framework. Level 4 represents Data Architecture, Application Architecture, and Technology Architecture (Ji & Xia, 2007).

The FEAF's primary goal is to ensure consistent information sharing between agencies and government organisations by providing a unified structure and management tool for federal agencies (Goethals, 2005). Although FEAF can meet the needs of most organisations, it is mainly a framework for architectural planning. FEAF has only limited support the non-functional requirements of an organisation, and the framework does not adequately consider the rationale of the design (Tang et al., 2004).

2.4. Why Choose TOGAF®?

EA and interoperability models are closely linked in e-government. EA is an approach to facilitate e-government and interoperability in particular (Janssen, 2012). It is regarded as an effective way to deal with interoperability conflicts (Pardo et al., 2012 as cited in Schekkerman, 2006) and to promote interoperability cross-agency (Pardo et al., 2012 as cited in Janssen & Kuk, 2006). Interoperability plays an important role to achieve the collaboration and integration of government services (Sedek et al., 2011). EAFs offer guidelines on how to use EA viewpoints in detail, while interoperability frameworks (IF) assist in classifying system concerns by using interoperability layers (Mondorf & Wimmer, 2016). The interoperability layers and architecture viewpoints have different purposes, but they have a similar approach, it is significant to establish a link between them (Mondorf & Wimmer, 2016).

In this section, a table comparing the frameworks based on previous literature shows which has the better interoperability performance in Technical, Semantic and Organisational aspects. As mentioned before, since DoDAF was developed specifically for the U.S. DoD to support their combat operations and is no longer used by the e-Government program (Mohamed et al., 2012), we excluded it from the comparison.

	Technical Interoperability	**Semantic Interoperability**	**Organisational Interoperability**
ZFEA™	Does not support Technical Interoperability (Mohamed et al., 2012)	Partially supports Semantic Interoperability (Mohamed et al., 2012) Offer a placeholder for semantic models; But no explicit semantic support to cover interactions with other organisations (Sanchez et al., 2007).	Partially supports Organisational Interoperability (Mohamed et al., 2012) Has the owner's perspective of the description of the organisation's business processes (Sanchez et al., 2007). No explicit place-holder for interactions across the borders of the organisation (Sanchez et al., 2007).
TOGAF®	Partially supports Technical Interoperability (Mohamed et al., 2012) "The Technology Architecture View provides a place-holder for the technical aspect." (Sanchez et al., 2007)	Partially supports Semantic Interoperability (Mohamed et al., 2012) The Information models offer semantic support for the organisation's business processes. (TOGAF® information model is available for semantic support for interaction with third parties (Sanchez et al., 2007).	Explicitly supports Organisational Interoperability (Mohamed et al., 2012) TOGAF® offers a clear business model that explicitly captures participants, relationships and roles and can be used to capture internal business processes (Sanchez et al., 2007). Some TOGAF® business models are used as place-holders for the purposes of collaborations involving third-party organisations and enable interaction purposes (Sanchez et al., 2007).
FEAF	Explicitly supports Technical Interoperability (Mohamed et al., 2012) Addresses Technical Interoperability issues through the TRM (Sanchez et al., 2007).	Partially supports Semantic Interoperability (Mohamed et al., 2012) The DRM is available to offer semantic support to the third-party organisations' interaction (Sanchez et al., 2007).	No place-holder describing participants, roles and relationships between business processes (Sanchez et al., 2007). No prescription for modelling of business processes (Sanchez et al., 2007).
DoDAF	Discontinued – excluded from this comparison.		

Table 1. Comparison of EAFs from an interoperability perspective

According to Table 1, TOGAF® has the best performance in the comparison of Technical, Semantic and Organisational interoperability aspects. One of the advantages of TOGAF® is that it can be designed as a generic framework, which means it can be used to develop many enterprise architectures and can be combined with any other

framework focused on a specific sector (Herdiana, 2018). In addition, TOGAF® has a less abstract level than the Zachman Framework™ and is unlike DoDAF which is tailored to a specific field (Sitton & Reich, 2015). It provides a strong basis for the process of system architecture design (Sitton & Reich, 2015). Another advantage is the integration of TOGAF® with ArchiMate®, which offers tools to support EA in the description, analysis and visualisation of the relationships among business domains (Mohamed et al., 2012).

TOGAF® explicitly supports Organisational Interoperability and partially supports Semantic Interoperability and Technical Interoperability (Tang et al., 2004). TOGAF® has a chapter that provides guidelines for interoperability requirements definition and establishment (The Open Group, 2018). Determination of interoperability is embedded throughout the TOGAF® ADM, which is represented in phases A - F (The Open Group, 2018). TOGAF®'s guidelines on Interoperability Requirements provide a way to formalise cross-organisational relationships (Mondorf & Wimmer, 2016). The consideration of interoperability was also conducted in the central phases (Requirements Management) of TOGAF® life-cycle models. For instance, the central phases of Risk Management and Project Management identify risks and complexities related to interoperability projects and efforts (Mondorf & Wimmer, 2016). However, because of the large scope of TOGAF®, it is essential to make serious customisation before applying it (Mondorf & Wimmer, 2016, as cited in The Open Group, 2011).

3. Case Study - Government of Canada

Some governments have adopted TOGAF® as a base reference framework for creating interoperability models or guidance to solve interoperability issues, such as The European Interoperability Reference Architecture (EIRA) (European Commission, 2017), Thailand (Suchaiya & Keretho, 2014), and the Government of Canada. The Government of Canada (GC) was chosen as a case study in this article.

3.1. The Government of Canada - EAF

GC conducts a TOGAF®-based EAF and has developed its interoperability model. GC's EAF mainly focuses on five sectors associated with TOGAF®: Business Architecture, Information Architecture, Application Architecture, Technology Architecture, and Security Architecture (TBCS, 2022a). The review of GC's EAF is as follows:

- Business Architecture: GC thinks that business architecture is key to successfully implementing GC's Enterprise Ecosystem Target Architecture. In this section, GC mainly focuses on an end-to-end digital design service that meets the requirements of GC's users and other stakeholders. Architects are results-oriented and strategically aligned with the department and GC to recognise opportunities for cohesion improvement. Additionally, GC tries to improve horizontal enablement of the enterprise to clearly understand reuse opportunities for cross-government.
- Information Architecture: GC conducts relevant practice to support the orientation of business service and business capability and effectively promote information and data sharing across the government. In addition, GC's information architecture should reflect responsible data and information management and governance practices, such as the source, interoperability, quality, etc. that are related to the data assets, as well as compliance with security and privacy requirements.
- Application Architecture: GC believes that the practice of application architecture must evolve significantly to successfully achieve the target architecture for their Enterprise Ecosystem. Interoperability becomes a significant factor and needs to be considered in the design of it: design highly modular and loosely coupled systems, expose services via API, and let APIs be discoverable to the appropriate stakeholders.
- Technology Architecture: GC thinks that the technology architecture must be aligned with its application architecture, technology architecture is an essential factor for solutions with high availability and adaptability. Therefore, in technology architecture, GC considers cloud adoption first and makes performance, availability and scalability a priority, while at the same time committing to the principles of DevSecOps.
- Security Architecture: IT security architecture helps GC ensure the implementation of the basic security modules when renewing infrastructure. It requires building security across all architectural layers, ensuring the accessibility of security to systems and services, and the maintenance of secure operations

In addition, GC identifies its Service and Digital Target EA which is also based on the TOGAF® framework (TBCS, 2022b). In the Service and Digital Target EA, there is a specific layer that describes the interoperability of services through standard structures, which are supported by API standards (TBCS, 2022b).

3.2. Government of Canada Interoperability Framework (GCIF)

GCIF Mission

A government interoperability framework is essential for the standardisation of information exchange. Based on the EA of the GC, a government interoperability framework is built to guide the construction of GC. This can lead to the robustness of interoperability and help the GC to build a transparent, efficient, and effective e-government.

GCIF Structure

The scope of GCIF is in line with TOGAF's® four architecture domains and is comprised of four perspectives of architecture: business, information, application and technology (see Figure 3). Each architecture corresponds to 4 goals: cross-domain interaction, common language, interconnected applications, and a common interoperability platform. Governance, security and privacy are emphasised across all the architectures. In the following section, each architecture of GCIF will be discussed in detail.

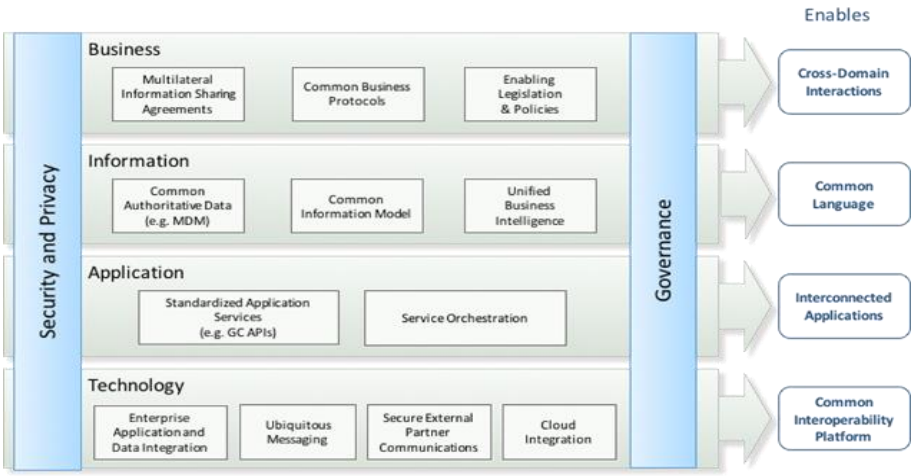

Figure 3. GC Interoperability (TBCS, 2017).

3.2.1. Business Architecture

According to TOGAF®, the business architecture defines the organisation's business strategy, core business processes and standards (The Open Group, 2018). The business architecture in GCIF enables the government to achieve cross-domain interactions. The common understanding of the information sharing agreements, business protocols and legislation ensure the other three architecture domains align with each other and allow cross-domain interactions. As a result, GC can seamlessly deliver its services.

3.2.2. Information Architecture

TOGAF® defines data architecture as describing an organisation's design of data assets and management (The Open Group, 2018). For GC, the information architecture helps the government EA to standardise the language. The outcome of a common language enables GC to exchange data in a seamless flow, which facilitates the efficiency and accuracy of the services delivered. It is noticeable that open data is one of the critical aspects of building a transparent government. The information architecture ensures the data assets of GC are transparent, open, and authoritative while safeguarded with security, privacy and confidentiality (TBCS, 2017).

3.2.3. Application Architecture

TOGAF® identifies the application architecture as a blueprint for deploying individual applications and guidelines for their interactions with business processes (The Open Group, 2018). This is in line with the goal of GCIF in the application domain, which is to build interconnected applications in government EA. As mentioned above, APIs are crucial for interconnection of applications from different departments and organisations. APIs allow individual applications to integrate with each other, delivering seamless services, while these applications can still be developed and maintained independently. This benefits EA since it is reusable, replaceable, and cost-effective.

3.2.4. Technology Architecture

The Technology Architecture describes the requirement of technology capabilities to support the deployment of the other three domains' services (The Open Group, 2018). This domain is key to achieving a common interoperability platform. Cloud computing is emphasised since it enables on-demand network access to shared computing resources (TBCS, 2017). This will be further discussed in the interoperability challenges faced by GC.

3.3. Interoperability Challenges of GC

The COVID-19 outbreak has tested the resilience of the Canadian government as never before. The transformation has become the new normal. In the face of COVID-19, governments around the world are restructuring their operations to save costs and improve efficiency by moving systems and applications to the cloud (Kuada et al., 2012). Managing government systems must ensure that technical liabilities are avoided by taking steps to ensure and maintain portability and interoperability, properly evaluating and adopting practices. (Irion, 2012).

Cloud and infrastructure are interrelated because the cloud is the infrastructure that ensures scalability, reliability, security, responsiveness, and more. Essentially, it involves payment and use of distributed low-cost hardware, and how to deal with interoperability issues in the cloud is a major challenge for Canadians (Canadian Center for Cyber Security, 2020).

3.3.1. Management complexity

Running a cloud requires a multi-party effort that requires the input of skills, people and time resources. Even seemingly simple resource allocation can be confusing if suppliers use different methods or indicators to measure efficiency. Besides, it is difficult to find experts who can span multiple cloud domains. Due to the inherent complexity of government systems, applications need to be reconfigured to fit specific clouds, as well as tools with mismatched functionality (Treasury Board of Canada Secretariat, 2018). If a large-scale migration effort is required to deploy across platforms to make applications on different clouds compatible with the corresponding API, multi-cloud will lose its original advantage. In order to circumvent this operational complexity, the most important thing is to follow the standardisation of related processes and reduce the attachment to related services that other cloud service providers cannot provide.

3.3.2. Security considerations

Multi-cloud platforms create a more likely environment for attacks and vulnerabilities, so more is required for effective security, governance, and compliance (Canada Center for Cyber Security, 2020). Today, cloud service providers implement a modern approach to digital asset protection. However, when it comes to a multi-cloud strategy, the primary responsibility lies with the government itself. It is important to have an in-depth discussion of security needs, how to avoid protection failures, and what to do about security breaches or data loss.

3.3.3 Redundancy, Backup, Disaster Recovery and Failover

Security-related policies such as disaster backup, data backup, etc. need to be considered, and the system should guarantee the possibility of automatic switching to the backup platform in the event of failure or complete unavailability of the primary cloud service. To avoid loss of data in transit, consider data synchronisation between applications running across a multi-cloud environment and the process of performing database updates between clouds with minimal latency.

3.4. How TOGAF® addresses the interoperability challenges

The interoperability challenges faced by GC are addressed by TOGAF® throughout the ADM. Each phase of the ADM has presented the determination of interoperability. The following sub-sections discuss which phases could specifically deal with each interoperability challenge.

3.4.1. Enhancing interoperability management

TOGAF® can mitigate the challenge of management issues through phases A, B, C and D. In phase A, the nature of the information and service exchanges among different business units were discovered and considered using the business scenarios technique (The Open Group, 2018). In phases B and C, the exchanges of information and services are further documented using corporate data and/or business models (The Open Group, 2018). How various applications or systems would share information and services is specified in these phases (The Open Group, 2018). In phase D, the technical mechanism to process information and service exchange is determined (The Open Group, 2018).

After going through the TOGAF® ADM cycle, the integration process would be standardised in terms of its tools and processes which helps reduce the complexity of ICT infrastructure in terms of interoperability management.

3.4.2. Improving data security

TOGAF® addresses the security consideration by implementing safety standards in all of its ADM phases. Each phase has considered the security requirements specifically and gives practical security policies to guide data security management (The Open Group, 2018). For instance, one of phase B's security policies indicates the importance of confirming the legitimate actors who would interact with different data (The Open Group, 2018). The people actors and system actors are common sources of data breaches, and human error has always been a vital subject of information security management (Evans et al., 2016). If those actors, such as backup operators, are not identified and managed, attackers may use the ambiguous authorisation standards to steal data from the systems.

3.4.3. Developing risk management

TOGAF® has a specific chapter on risk management regarding EA implementation. TOGAF® identified five activities for risk management: Risk Classification, Risk Identification, Initial Risk Assessment, Risk Mitigation And Residual Risk Assessment, and Risk Monitoring (The Open Group, 2018). The Risk Mitigation section pointed out that the mitigation efforts could vary from simple monitoring to a complete contingency plan (The Open Group, 2018). The risk management process is determined in the ADM. For example, phase G of the TOGAF® ADM conducts risk monitoring and is also able to identify critical risks that cannot be directly mitigated (The Open Group, 2018). In this case, another full or partial ADM cycle is required.

4. Conclusion

This paper highlights the importance of building government interoperability for e-government service delivery. We believe that a well-established EA can help to solve the key interoperability challenges faced by governments. By comparing four EAFs, we found that TOGAF® is the most suitable and adaptive framework to help governments establish a framework for interoperability.

Although this paper provides a conceptual and literature review to discuss the feasibility of EAFs for government interoperability, there are some limitations due to the scope and narrative of the paper. First, only four frameworks were studied to compare the guidance of different frameworks for EA and interoperability, and the remaining frameworks were not included in the discussion. Additionally, this paper only discusses three main interoperability issues faced by governments, while other issues remained uncovered in this study. Finally, this paper is theory-based and focuses on conceptual and theoretical research. Although the case of the Canada Government is studied and supported our research, the research lacks quantitative results and provides no implementation guidelines. Future studies can focus on the research areas of 1) a detailed review of different EAFs; 2) different interoperability issues; and 3) investigating different cases for quantitative results.

References

Carr, D., & Else, S. (2018). State of enterprise architecture survey: Results and findings. *Enterprise Architecture Professional Journal.*

Canada Center for Cyber Security. (2020). ITSP.50.103 Guidance on Security. https://cyber.gc.ca/en/guidance/guidance-security-categorization-cloud-based-services-itsp50103#annb

European Commission. (2017). *How does the EIRA support interoperability?* Retrieved 07 July 2022 from https://joinup.ec.europa.eu/sites/default/files/document/2017-01/how_does_eira_support_interoperability_v1_0_0.pdf

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, *9*(17), 4667-4679. https://doi.org/10.1002/sec.1657

Gerber, A., Roux, P. L., Kearney, C., & Merwe, A. V. D. (2020). *The zachman framework for enterprise architecture: An explanatory is theory*. Springer, Cham, Switzerland.

Goethals, F. (2005). An overview of enterprise architecture framework deliverables. *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.870207

Goldkuhl, G. (2008). *The challenges of Interoperability in E-government: Towards a conceptual refinement*. Paper presented at the Pre-ICIS 2008 SIG eGovernment Workshop, Paris, France.

Gottschalk, P. (2009). Maturity levels for interoperability in digital government. *Government Information Quarterly*, *26*(1), 75-81. https://doi.org/10.1016/j.giq.2008.03.003

Herdiana, O. (2018). TOGAF ADM planning framework for enterprise architecture development based on health minimum services standards (HMSS) at Cimahi city health office. Paper presented at the IOP Conference Series: Materials Science and Engineering, Bandung, Indonesia.

Irion, K. (2012). Government cloud computing and national data sovereignty. *Policy & Internet*, *4*(3-4), 40-71. https://doi.org/10.1002/poi3.10

Janssen, M. (2012). Sociopolitical aspects of interoperability and enterprise architecture in E-Government. *Social Science Computer Review*, *30*(1), 24-36. https://doi.org/10.1177/0894439310392187

Janssen, M., Charalabibis, Y., Kuk, G., & Cresswell, T. (2011). Guest editors' introduction: E-government interoperability, infrastructure and architecture: State-of-the-art and challenges. *Journal of Theoretical and Applied Electronic Commerce Research*, *6*(1), I-VIII. https://doi.org/10.4067/S0718-18762011000100001

Ji, W., & Xia, A. (2007). Federal enterprise architecture framework. *Computer Integrated Manufacturing Systems-Beijing*, *13*(1), 57-66.

Jiménez, C. E., Solanas, A., & Falcone, F. (2014). E-Government interoperability: Linking open and smart government. *Computer*, *47*(10), 22-24. https://doi.org/10.1109/MC.2014.281

Kuada, E., Olesen, H., & Henten, A. (2012). *Public policy and regulatory implications for the implementation of opportunistic cloud computing services for enterprises*. Paper presented at the 9th International Workshop on Security in Information Systems, Wroclaw, Poland.

Lallana, E. C. (2007). E-Government interoperability: A review of government interoperability frameworks in selected countries. *United Nations Development Programme (UNDP)*, *17*, 2009.

Lau, J. T. F., Yeung, N. C. Y., Choi, K. C., Cheng, M. Y. M., Tsui, H. Y., & Griffiths, S. (2010). Factors in association with acceptability of A/H1N1 vaccination during the influenza A/H1N1 pandemic phase in the Hong Kong general population. *Vaccine*, *28*(29), 4632-4637. https://doi.org/10.1016/j.vaccine.2010.04.076

Mohamed, M. A., Galal-Edeen, G. H., Hassan, H. A., & Hasanien, E. E. (2012). *An evaluation of enterprise architecture frameworks for e-government*. Paper presented at the Seventh International Conference on Computer Engineering & Systems (ICCES), Cairo.

Mondorf, A., & Wimmer, M. A. (2016). *Requirements for an architecture framework for Pan-European e-government services*. Paper presented at the International Conference on Electronic Government, Guimarães, Portugal.

Novakouski, M., & Lewis, G. A. (2012). *Interoperability in the e-Government Context: Defense Technical Information Center*. Pittsburgh, PA: Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.

Oliveira, A. D. A., & Eler, M. M. (2017). Strategies and challenges on the accessibility and interoperability of e-government web portals: A case study on Brazilian federal universities. Paper presented at the IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Turin, Italy.

Pardo, T. A., Nam, T., & Burke, G. B. (2012). E-Government interoperability. *Social Science Computer Review*, *30*(1), 7-23. https://doi.org/10.1177/0894439310392184

Perks, C., & Beveridge, T. (2003). *Guide to enterprise IT architecture*. Springer, New York, NY, USA.

Sanchez, A., Basanya, R., Janowski, T., & Ojo, A. (2007). *Enterprise architectures-enabling interoperability between organizations*. Paper presented at the 36th Argentine Conference on Informatics 8th Argentinean Symposium on Software Engineering, Mar del Plata, Argentina.

Sedek, K. A., Sulaiman, S., & Omar, M. A. (2011). *A systematic literature review of interoperable architecture for e-government portals*. Paper presented at the 2011 Malaysian Conference in Software Engineering, Johor Bahru, Malaysia.

Sitton, M., & Reich, Y. (2015). Enterprise systems engineering for better operational interoperability. *Systems Engineering*, *18*(6), 625-638. https://doi.org/10.1002/sys.21331

Suchaiya, S., & Keretho, S. (2014). *Analyzing national e-Government interoperability frameworks: A case of Thailand*. Paper presented at the Ninth International Conference on Digital Information Management (ICDIM 2014), Phitsanulok, Thailand.

Sulehat, N. A., & Taib, D. C. A. (2016). E-Government information systems interoperability in developing countries. *Journal of Business and Social Review in Emerging Economies*, *2*(1), 49-60. https://doi.org/10.26710/jbsee.v2i1.18

Tamm, T., Seddon, P. B., Shanks, G., & Reynolds, P. (2011). How does enterprise architecture add value to organisations? *Communications of the Association for Information Systems*, *28*(1), 141-168. https://doi.org/10.17705/1CAIS.02810

Tang, A., Han, J., & Chen, P. (2004). *A comparative analysis of architecture frameworks*. Paper presented at the 11th Asia-Pacific software engineering conference, Busan, Korea (South).

The Open Group. (2018). *Welcome to the TOGAF® Standard, Version 9.2, a standard of the Open Group*. Retrieved 11 July 2022 from https://pubs.opengroup.org/architecture/togaf92-doc/arch

Treasury Board of Canada Secretariat (TBCS). (2017). *GC Interoperability Maturity Model*. Retrieved 11 July 2022 from https://open.canada.ca/ckan/en/dataset/922cf2be-bedc-5ed6-b26a-c27b79685915

Treasury Board of Canada Secretariat (TBCS). (2022a). *Government of Canada enterprise architecture framework*. Retrieved 04 July 2022 from https://www.canada.ca/en/government/system/digital-government/policies-standards/government-canada-enterprise-architecture-framework.html

Treasury Board of Canada Secretariat (TBCS). (2022b). *Service and digital target enterprise architecture white paper*. Retrieved 08 July, 2022 from https://www.canada.ca/en/government/system/digital-government/policies-standards/service-digital-target-enterprise-architecture-white-paper.html

U.S. DoD Architecture Framework Working Group. (2010). *The DoDAF Architecture Framework Version 2.02*. Retrieved 10 July 2022 from https://dodcio.defense.gov/library/dod-architecture-framework

Xuemin, Z., Zhiming, S., & Ping, G. (2012). The process of information systems architecture development. *Procedia Engineering*, *29*, 775-779. https://doi.org/10.1016/j.proeng.2012.01.040

Zachman, J. A. (2009). *The concise definition of the zachman framework by: John a. Zachman*. Retrieved 07 July 2022 from https://www.zachman.com/about-the-zachman-framework