Implementing Cybersecurity In DefTech Sdn Bhd using DoDAF

Yunnyzar Mohd Zain[1], Nur Sabrina Syazwani Mazlan[2], Nur Azaliah Abu Bakar[3], Surya Sumarni Hussien[4]

[1,2]Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia
[3]Faculty of Computer and Mathematical Sciences, Universiti Teknologi Mara

[1]yunnyzar@graduate.utm.my, [2]azaliah@utm.my, [3]suryasumarni@uitm.edu.my,

Article history

Received: 13 May 2023
Received in revised form: 18 June 2023

Accepted: 23 June 2023

Published online: 27 June 2023

*Corresponding author amnasakinah@graduate.utm.my

Abstract

A company's architecture significantly affects how much it is worth. Enterprise Architecture (EA) is the term used to describe the ideas and standards that guide the execution of information, technology, and business mission in defence companies. The main objective is to align information technology and business strategy better. For this project, we selected Defence Technologies Sdn Bhd (DefTech) for the case study in implementing the EA. the purpose of this research is to include the as-is and to-be scenarios in detail of each division in the organisation by using DoDAF. DefTech is in the security and defence industry. The main aim is to implement Cybersecurity for data security and asset planning since they supply and produce armoured and logistic vehicles specifically for military and homeland security. The As-Is and To-Be scenarios for DefTech were explained, and data leak protection has been added as the future architecture for the organisation. The component will increase cybersecurity protection and traceability during data leakage. Implementing and enforcing a DoDAF standard reduces inefficiencies in enterprise security and identifies weaknesses. EA has shown potential utility for designing integrated architectures for a business on its own. Still, it can also act as the hub for other initiatives to govern the collaborative enterprise, particularly those centred on security.

Keywords: *Enterprise architecture, DoDAF, EA framework, defence, security*

1. Introduction

An increasing number of corporations and public sector actors have recognised the importance of Enterprise Architecture (EA) to enterprise transformation. The architecture of a company has a substantial impact on its worth. EA refers to the concepts and criteria that govern the implementation of information systems, technology, and business mission in defence enterprises, referred to as enterprise architecture which is the primary goal to improve the alignment of information technology and business strategies.

The application of an enterprise architectural framework is required to achieve assurance against current and potential cyber threats. To provide crucial system interoperability, cooperative information sharing, information assurance, and trust, enterprise architectural frameworks offer important technical reference models for system design and maintenance. The efficient planning and acquisition of modern communication systems and the maintenance of secure enterprise networks depend on enterprise architectural frameworks.[9]

The architecture shapes the enterprise's capabilities and behaviour to a considerable extent. Enterprise engineering, or designing an enterprise, is a system engineering technique for establishing the required enterprise capabilities and designing the structure, processes, information, and technology to deliver those capabilities. [13] Nonetheless, existing EA models and frameworks appear incapable of reflecting military organisations' dynamic and expansive nature. Architects may benefit from a better grasp of the evolution of enterprise structures through time as they design military reforms [5].

For this project, we selected Defence Technologies Sdn Bhd (DefTech) for the case study in implementing the EA. DefTech is a wholly owned subsidiary of DRB-HICOM and was incorporated to contribute to Malaysia's industrialisation and self-reliant defence aspirations. DefTech is one of the Malaysian defence contractors that develops, manufactures, and supplies armoured and logistic vehicles for military and homeland security. In addition to specialised vehicles and commercial buses, DefTech is a supplier of both. They are the ones who manufactured and supplied the ACV-300 Adnan family of vehicles to the Ministry of Defence as well as Gempita in 2014. After acquiring Composites Technology Research Malaysia, DefTech achieved a significant milestone in the aerospace and unmanned aerial vehicle industries (CTRM). Defence Technologies, Defence Services, DefTech Systems Integration, DefTech Unmanned Systems, and DefTech Aviation are among the DefTech divisions [10]. DefTech needs to implement EA in their company to assist them in management and asset management.

Accordingly, we selected The Department of Defense Architecture Framework (DoDAF) as the framework constructed based on the defence industry. DoDAF is a set of guidelines for showing, characterising, and comparing Department of Defense (DoD) enterprise architectures across organisational, joint, and international lines. It fosters the use of common jargon, assumptions, and ideas to make integration easier. As a result, DoDAF is highly suited to large systems with complex integration and interoperability challenges and uses "operational perspectives" uniquely. These views give a high-level overview and details for specific stakeholders within their domains and interfaces with other domains where the system will be used [11].

The rest of this study begins with a survey of scholarly literature on digital platforms, information infrastructures, and path construction. The case data and an overview of DefTech's ongoing digitalisation journey show how DefTech is gradually using EA management to transform its information infrastructure into a digital platform. The analysis that follows offers a path constitution viewpoint on this process. The paper ends with findings and conclusions.

2. Literature Review

This section will introduce Enterprise Architecture (EA) and the Department of Defense Architectural Framework (DoDAF) understanding based on previous research and studies.

2.1 Enterprise Architecture (EA)

A desired-to-be EA is implemented through a series of small projects, gradually getting the company closer to the target architecture. There are numerous potential initiatives, and the challenge is chosen to pursue given funding and time constraints [1]. To provide crucial system interoperability, cooperative information sharing, information assurance, and trust, enterprise architectural frameworks offer important technical reference models for system design and maintenance. EA affects the efficient planning and acquisition of modern communication systems and the maintenance of secure enterprise networks [9].

2.2. Department of Defense Architectural Framework

The Department of Defense Architectural Framework (DoDAF) is used by the Department of Defense of the United States of America to create and document its massive and complex EA. It has grown into a large and varied topic matter. It is an EA framework developed to model big and complex companies and systems where interoperability and integration are problematic [12].

A study [1] proposed a real-options framework for planning a project portfolio to achieve a desired corporate architecture. They offer a way of defining projects as a set of real compound options using DoDAF. The capability phasing perspective of DoDAF v2.0 was determined using a switching model and Monte Carlo simulation. To demonstrate that approach, a case study of a modest defence contractor has been done. The model and method provide a method for valuing a portfolio of projects to create an EA. The systems engineering tools were created to assist the Department of Defense (DoD) in realising its net-centric transformation to have more effective and efficient war- fighting capabilities is the driving force behind this research.

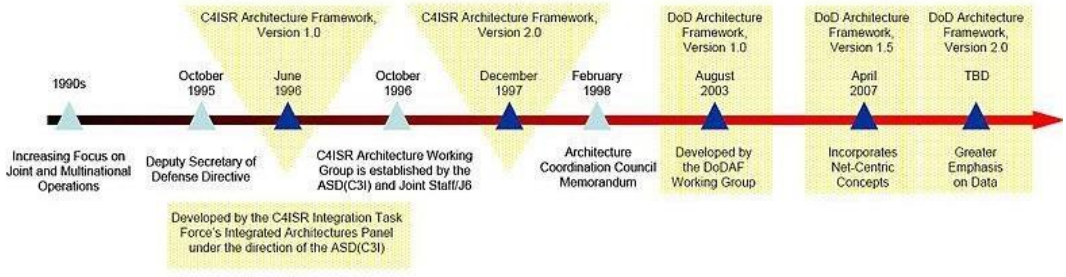

Figure 1. Evolution of the DoDAF [10]

From C4ISR to DoDAF, such an enterprise architectural framework to describe concepts and models useable in DoD's key processes has significantly evolved in the EA. DoDAF accomplishes this by supplying views to describe the DoD's complex operations, allowing an architecture description's broad scope and intricacies to be visualised, understood, and assimilated. DoDAF can deduce the necessary components and concepts to implement security needs despite the lack of a dedicated security viewpoint [3].

3. Methodology

The case study of this research is DefTech, and the purpose of this research is to include the as- is and to-be scenarios in detail of each division in the organisation using DoDAF. DefTech is in the security and defence industry. The main aim is to implement Cybersecurity for data security and asset planning since they supply and produce armoured and logistic vehicles specifically for military and homeland security. DefTech is renowned for its superior overhauling and maintenance of land systems, and it recently expanded its scope to include aerospace, composite structures, unmanned systems, and system integration.

Through strategic cooperation with many stakeholders, its long-term aim is to develop an indigenous land fighting system and airborne surveillance, control, and combat system. DefTech's goal is to become Malaysia's best and most complete defence contractor. The internal coherence inside one organisation was the fundamental motivator for enterprise design in the industry, focusing on cost-effectiveness by minimising redundancies. This necessitates enterprise-wide interoperability and the standardisation of numerous procedures and technologies. The focus has shifted from efficiency to agility to speed up change and time to market. DoDAF will add real value to the company as it gives a clear picture of a specific view of the business activity.

3.1. Implementing DoDAF as Enterprise Architecture Framework

The DoD uses DoDAF to define a system's architecture. An article [3] compiles details explaining DoDAF. It contributes a high-level overview and introduction to DoDAF, including essential vocabulary, concepts, development processes and its use in handling enterprise security planning issues. The study stated that DoDAF is specifically built to address the DoD's six primary processes, which are:

a. Joint Capability Integration and Development System (JCIDS)
b. Defense Acquisition System (DAS)
c. System Engineering (SE)
d. Planning, Programming, Budgeting, and Execution (PPBE)
e. Portfolio Management (PfM)
f. Operations

In the latest version of this framework that was published in 2009, namely DoDAF v2.0, there are a few crucial terminologies to be aware of to comprehend the framework: [8] fully

a. Models: The 'products' specified in prior versions of DoDAFand to visualise the architectural data. Models might be texts, spreadsheets, dashboards, or other graphical visuals, which are used to organise and show data in a more understandable manner
b. Views: A view is created when data is gathered and presented in a model format
c. Viewpoints: Organised collections of points of view typically representing processes, systems, services, standards, etc.

The DoDAF process's documented results are divided into the following Viewpoints or Architecture Types:

a. Capability Viewpoint (CV)
b. Operational Viewpoint (OV)
c. Services Viewpoint (SvcV)
d. Systems Viewpoint (SV)
e. Project Viewpoint (PV)
f. Standards Viewpoint (StdV)
g. Data and Information Viewpoint (DIV)
h. All Viewpoint (AV)

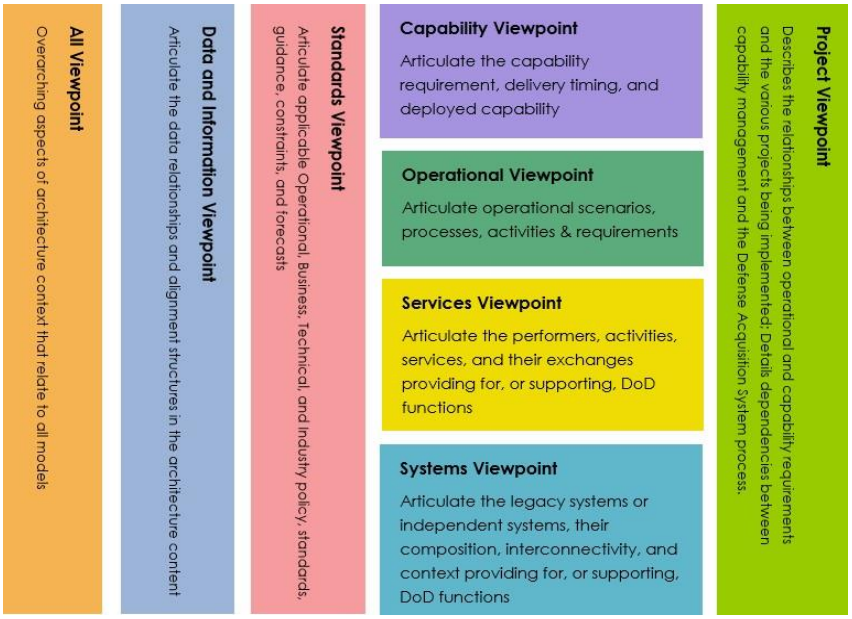

Figure 2 DoDAF v2.0 – The Architecture Viewpoints[11]

4. Result and Discussion

Implementing Cybersecurity by using DoDAF into DefTech will be explained using the As-Is and To-Be scenarios in the ArchiMate notation, as shown in Figure 3 and Figure 4, respectively. Data leak protection has been added as the future architecture for the organisation. The component will increase cybersecurity protection and traceability during data leakage.

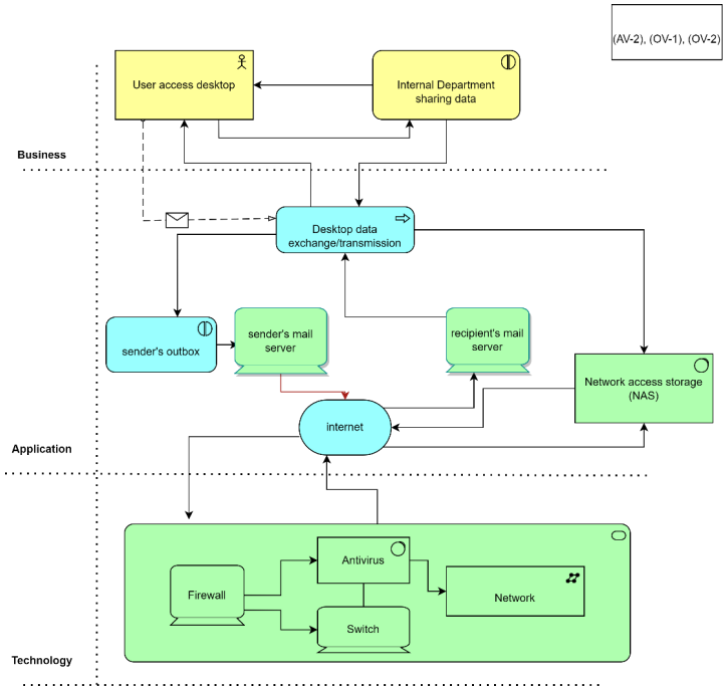

Figure 3 As-Is Scenario of DefTech

5. Conclusion

In conclusion, this research implemented DoDAF as the framework to build Cybersecurity into DefTech. Data leak protection has been added to the organisation's future architecture, and the As- Is and To-Be scenarios for DefTech have been described. The element will improve cybersecurity defences and data leak tracing. Enterprise designs may be effectively communicated, and collaboration between organisational and coalition stakeholders can be increased by integrating DoDAF into system development life cycles. The relevance of the stakeholders is improved by utilising technologies that rely on effective data gathering and quality. Policies would also guarantee consistent and accurate architectural viewpoints and automatic viewpoint formation. Implementing and enforcing a DoDAF standard reduces inefficiencies in enterprise security and identifies weaknesses. EA has shown potential utility for designing integrated architectures for a business on its own. Still, it can also act as the hub for other initiatives to govern the collaborative enterprise, particularly those centred on security.

Acknowledgement

This research was funded by a grant from UTM (R.K130000.7756.4J574).

References

[1] R. E. Giachetti, "A Flexible Approach to Realise an Enterprise Architecture," in Procedia Computer Science,2012, vol. 8, pp. 147–152. doi: 10.1016/j.procs.2012.01.031.

[2] M. Hue, "A Review of Enterprise Architecture Use in Defence," 2014.

[3] L. Ertaul and J. Hao, "Enterprise Security Planning with Department of Defense Architecture Framework (DODAF)."

[4] Defense Security Enterprise Architecture, "Product Reference Guide," 2016.

[5] J. Mattila and S. Parkinson, "Enterprise Architecture as a Tool in Military Change Management."

[6] C. P. David Brown, "Enterprise Architecture for DoD Acquisition," 2000.

[7] "MALAYSIA'S NATIONAL DEFENCE POLICY."

[8] "DoDAF Architecture Framework Version 2.02 Home DoDAF-DM2 WG DoDAF Journal DoD Meta Data Registry IDEAS Links The DoDAF Architecture Framework Version 2.02." [Online]. Available: http://cio- nii.defense.gov/sites/dodaf20/index.html[

[9] D. Vance and A. Vance, "Securing Enterprise Architecture with the Department of Defense Architectural Framework (DoDAF); Improving Cybersecurity with DoDAF Fit-for-Purpose Views," 2016. [Online].
Available: https://www.researchgate.net/publication/333774115

[10] "Department of Defense Architecture Framework - Wikipedia." https://en.wikipedia.org/wiki/Department_of_Defense_Architecture_Framework

[11] "What is DoDAF Framework." https://www.visual-paradigm.com/guide/enterprise- architecture/what-is-dodaf-framework/

[12] "DODAF - DOD Architecture Framework Version 2.02 - DOD Deputy Chief Information Officer."https://dodcio.defense.gov/Library/DoD-Architecture-Framework/]/

[13] "What is enterprise architecture? A framework for transformation."https://www.cio.com/article/222421/what-is-enterprise-architecture-a-framework-for- transformation.html