How can organisations effectively apply enterprise architecture frameworks to enhance cybersecurity resilience?

Jiawei Tong
University of Melbourne
jiaweitong1998@gmail.com

Jiayuan Zhang
University of Melbourne
jiaynzhang@gmail.com

Xinlan Chen
University of Melbourne
alanna0086@gmail.com

Qianqing Lu
University of Melbourne
lilianalu52@gmail.com

Qiaoan Zhang
University of Melbourne
zqa1125135910@gmail.com

Rod Dilnutt
University of Melbourne
rpd@unimelb.edu.au

Abstract

Since cyber-attacks receive increasing attention in the current business environment, improving cybersecurity resilience has become one of the key objectives of many organisations' strategic plans. Some widely used Enterprise Architecture (EA) frameworks play a role as a reference standard for enterprises to improve their cybersecurity resilience, such as the Zachman Framework and the Open Group Architecture Framework (TOGAF), both of which provide a systematic approach to the security management of information systems. This paper points out the challenges that enterprises may face in cybersecurity and deeply analyses how EA frameworks are implemented in the assessment and enhancement of data control systems. By examining and analysing the existing literature on the subject and the concrete implementation of cybersecurity frameworks in real-life enterprise cases, this paper provides insight into the importance of an Enterprise Architecture Framework (EAF) in cybersecurity management, as well as a tabular summary of the core benefits and potential limitations of common EAFs. Our findings indicate that an EAF can help organisations refine cybersecurity establishment and build strategic plans based on actual security needs alignment. However, organisations should also be aware that an EAF is not a complete solution, which means that organisations need to incorporate other policies and applications when trying to solve specific security problems, with the insights provided by the EAF.

1. Introduction

Cybersecurity has long been a concern for global organisations (Ahmad et al., 2019). As cyberattacks become more prevalent, improving the resilience of their own cybersecurity has become a top priority for many organisations (Haughey, 2020). However, most organisations have faced a huge challenge when establishing an effective cybersecurity system, and that is, the complexity. Enterprises ought to consider multiple aspects including the availability of corresponding technologies, the governance structure of the organisation, and even the corporate culture when implementing or improving their cybersecurity systems. In this context, the Enterprise Architecture (EA) framework provides a promising solution and pathway to address this dilemma, which effectively facilitates standardisation and integration between different organisational elements (Chmielecki et al., 2014).

EA takes a holistic view of an organisation’s processes and aligns the business in a structured manner to help organisations better manage organisational structures (Koenen, 2015). An EAF also has sufficient potential to help organisations achieve process standardisation, integration of infrastructure and technology, and cybersecurity resilience. This allows organisations to choose to use the EAF as the basis of their strategy to design and build effective cybersecurity systems.

Despite the increasing trend of EAF adoption, little is known about how to effectively apply these frameworks to improve cybersecurity resilience, especially in real-world business environments. Thus, one research question arises: ***How can organisations effectively apply enterprise architecture frameworks to enhance cybersecurity resilience?***

The purpose of this paper is to illustrate how organisations can use the EA framework to improve their resilience in cybersecurity. This paper reviews the relevant literature and case studies of EA applied to cybersecurity and selects three real-world cases for comparison and in-depth analysis using data control as the point of penetration. This will not only provide a more intuitive and practical explanation for organisations but also stimulate further research and discussion on the capabilities and viability of EA cybersecurity.

2. Theoretical Foundation

First, we will deliver the theoretical foundation of the Enterprise Architecture (EA) framework to provide a high-level view of the organisation's business. This will provide the organisation with an understanding of how to select the appropriate EA Framework or its integration with other tools to define and, to some extent, address the organisation's security needs for subsequent activities that lead to improved enterprise security resilience.

2.1 Enterprise Architecture (EA) Framework

The Enterprise Architecture (EA) Framework provides a high-level perspective to define IT systems and business processes, and the relationships and interactions between them, with the extent to which the system and the process is shared by different components of the enterprise (Tamm et al., 2011). Its purpose is to assist organisations in planning and building blueprints for large-scale enterprise-level application architectures to achieve their future business goals and roadmaps from the as-is state to the to-be state (Gillis, 2023). Some of the most used EA frameworks include the Zachman Framework, TOGAF (The Open Group Architecture Framework), DoDAF (Department of Defense Architecture Framework), Gartner's Pace-Layer Framework and FEAF (Federal Enterprise Architecture Framework), among others. It is worth noting that the benefits of using EA Frameworks usually become apparent as the complexity and diversity of the organisation architecture increases (Gillis, 2023).

2.2 Zachman Framework

The Zachman Framework is one of the first EA frameworks, created by J.A. Zachman in 1987 (Koenen, 2015). The framework consists of a 6x6 matrix that provides a comprehensive system view, methodically gathering system-specific information from different perspectives (Koenen, 2015). The columns of the matrix represent fundamental questions related to architecture development that help identify the 5W1H that needs to be considered at various levels of the enterprise (Zachman, 1997). The rows of the matrix indicate different perspectives that define the topics and level of detail to answer the questions (Zachman, 2003). The Zachman Framework can be applied at any level of abstraction in the system development process and provides a degree of freedom for the modeller to make the system model more concrete. For companies with existing operating systems, the Zachman Framework for Information Systems Architecture (ISA) can be further adopted to define and control the logical structure of interfaces and integration of all components of the system (Ramadan & Hefnawi, 2007).

2.3 The Open Group Architecture Framework (TOGAF®)

The Open Group Architecture Framework (TOGAF) is a framework product developed by The Open Group (2011) that provides a standard approach to the development and management of EA (Koenen, 2015). Its value is recognised by IT stakeholders through its structured approach and clear guidelines that guide organisations to focus on aspects they may have overlooked, improve agility, and provide an organised approach to developing EA, thus assisting organisations to improve IT projects and facilitate their strategic development (Bhatia et al., 2023).

TOGAF provides an organisational architecture design and development methodology, the Architecture Development Methodology (ADM), and distinguishes three levels: business architecture, information systems architecture, and technical architecture (Rezaie et al., 2022). The ADM is one of the most powerful features of TOGAF and is highly adaptable and flexible (Koenen, 2015). The ADM describes which phases should be performed during the architecture development process and which artefacts and deliverables should be created to build a sound and complete architecture. It also defines several phases before and after the actual creation of the architecture (Koenen, 2015). Additionally, it provides guidance for the delivery of the architecture, leaving it up to the architects of a given project to decide on the breadth of coverage, level of detail, or timeframe, which is quite different from other frameworks such as Zachman Framework (Koenen, 2015). In a word, the Zachman framework is conceptual and describes how to categorise artefacts, while TOGAF is practical and guides organisations on how to do it (Sessions, 2007). Thus, the two frameworks can be used in a complementary way.

2.4 Cybersecurity Resilience

Cybersecurity resilience is the ability of an enterprise to quickly adapt and continue operations while preventing, detecting, controlling, and recovering from cyber threats (Haughey, 2020). A resilient cybersecurity strategy is critical to an organisation's operations while protecting against security threats and preventing data breaches and other enterprise cybersecurity threats (Haughey, 2020). The cybersecurity resilience framework consists of five key pillars:

identify, protect, detect, respond, and recover (Haughey, 2020). A cyber-resilient architecture should be achieved through a process of identifying all assets, risk assessment, selecting and evaluating assets, adopting resilience in the architecture, testing performance, establishing recovery processes, and continuous evolution (Conklin et al., 2017). Effective implementation of a cyber-resilient EA requires not only a strategic vision, but also daily involvement of the entire enterprise and should not be left to the security team alone (Haughey, 2020). It requires a holistic approach involving people, processes, and technology to ensure and optimise that vision (Conklin et al., 2017).

2.5 Data Control Systems

Data control systems are considered one of the ways to help create cybersecurity (Monino, 2020). Regulating data access is an important component of data control, which includes maintaining data security, providing access to critical data assets, managing permissions, and systems for managing and protecting organisational data assets (Ovaledge, 2021). To ensure the security and compliance of data assets, security management should be considered as a continuous improvement process, including activities such as risk monitoring and assessment, which should be conducted on a regular basis (Chmielecki et al., 2014). Moreover, continuous monitoring processes are required to maintain an up-to-date understanding of the effectiveness of risk response to assess risks, detect changes in processes and assets, and identify cybersecurity incidents (Chmielecki et al., 2014).

Additionally, data monitoring for business and IT requires a holistic view of the enterprise. As the carrier of system analysis, design and communication, EA is also a potential support for control system management (Ekstedt & Sommestad, 2009).

3. Challenges

Currently, enterprise cybersecurity is facing multiple challenges. The rapid evolution of technology under the dynamic business environment may cause enormous network security issues and distract organisations from their strategic plans (Boehm et al., 2022). Besides, the diverse cultures and business models of different companies lead to distinct network security requirements (Jalaliniya & Fakhredin, 2011). The frequent attacks and breach of security protocols from hackers considerably increase the difficulty in governing data systems and addressing cybersecurity issues (Buschle, 2014). The four main challenges faced by enterprise in data security are categorised as follows:

3.1 Data Control as a Foundation of Cybersecurity

Monino (2020) proposed that data control is one of the key aspects to ensure cybersecurity in the digital age. The implementation of a data control system should cover data access, data monitoring, and holistic data view. The organisation should consistently regulate the access to different types of data, monitor data to respond to any security breaches, and establish comprehensive insights of data, such as its sources and utilisation.

3.2 Agility of the Security System

The security system must be adaptable for companies to swiftly modify or update in response to the complexity in security threats which are caused by business changes or technological evolutions. The system should contain the capability for rapid evaluation and be responsible for responding to various cybersecurity incidents (Naseer et al., 2021).

3.3 Standardisation of Security System Implementation

The security system must respect and follow the data sovereignty laws based on the regions where the organisation operates. The data should be compatible across a variety of applications and platforms. There should be standardised protocols to cultivate a collaboration culture and integration among diverse aspects, such as technology and politics. For instance, when a cloud provider spreads to new regions, it should consider and address both technical challenges and the local policies that greatly influence data security (Alghamdi et al., 2021).

3.4 Transparency of the Security Policy

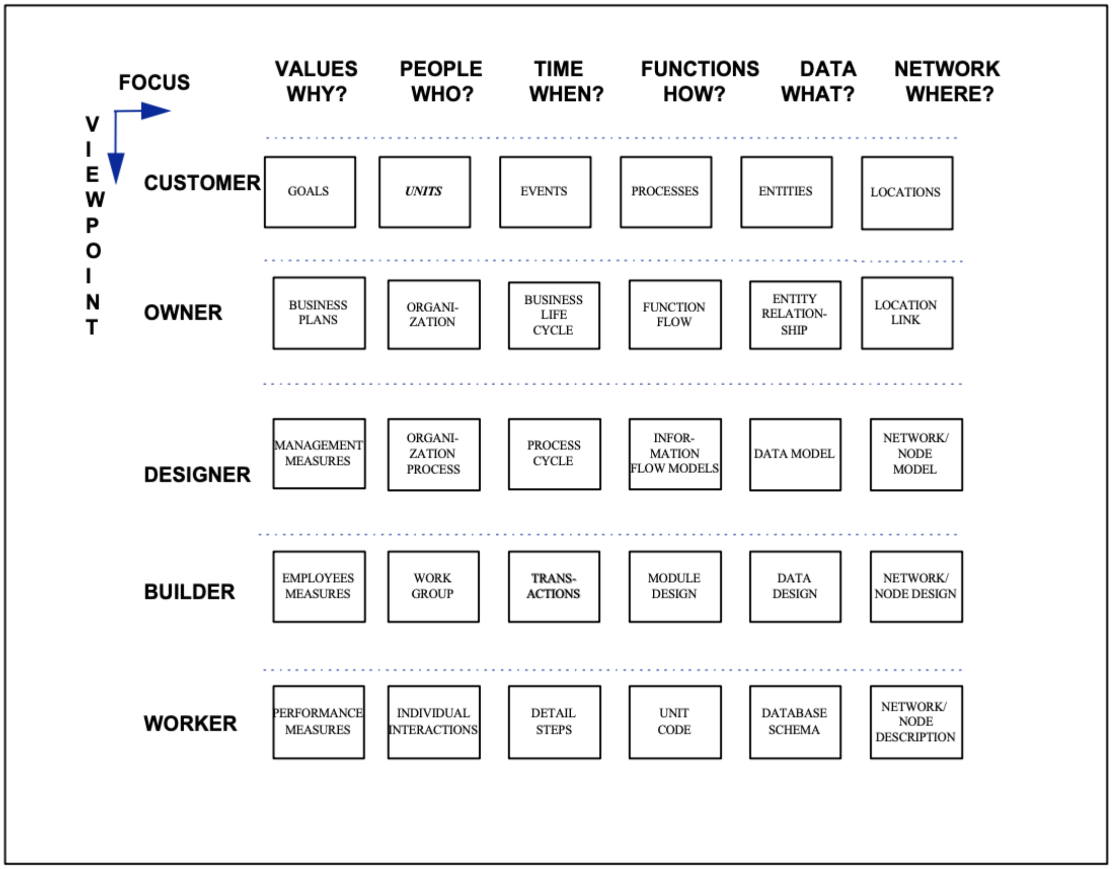
The security policy must ensure coherent integration between systems to facilitate communication and data exchange. The construction process of the policy should also be transparent and actively involve stakeholders within all organisational levels to reduce the chance of non-compliance (Larno et al., 2019). Regular audits of data access permissions are crucial to ensure that sensitive information is only visible to personnel with authority.

4. Case Analysis

4.1 Case 1 Harris Corporation

Harris Corporation is a technology company that is facing the challenge of creating an information system reengineering strategy to define the current system and target system and provide a transformation roadmap to align the user’s anticipations with these systems (Henning, 1996). Its Information Systems Division is required to devise an organisational information system reengineering methodology based on the Zachman framework (Oda et al., 2009). To automate and assist the development of Zachman cell structures, a middleware application is designed by Harris. This tool organises all the requirements and collectively reflects its current systems and emerging alternatives. The application simplifies requirement management without affecting its existing engineering discipline (Henning, 1996).

The Zachman framework is applied to Harris Corporation’s security engineering modelling, which models the security policy and offers an architecture for security management (Henning, 1996; Oda et al., 2009). Conforming to Harris’s system structure, the framework is reshaped and mainly focuses on Information System Architecture. The five layers include: customer, owner, designer, builder, and worker.



	VALUES WHY?	PEOPLE WHO?	TIME WHEN?	FUNCTIONS HOW?	DATA WHAT?	NETWORK WHERE?
CUSTOMER	GOALS	*UNITS*	EVENTS	PROCESSES	ENTITIES	LOCATIONS
OWNER	BUSINESS PLANS	ORGANIZATION	BUSINESS LIFE CYCLE	FUNCTION FLOW	ENTITY RELATIONSHIP	LOCATION LINK
DESIGNER	MANAGEMENT MEASURES	ORGANIZATION PROCESS	PROCESS CYCLE	INFORMATION FLOW MODELS	DATA MODEL	NETWORK/ NODE MODEL
BUILDER	EMPLOYEES MEASURES	WORK GROUP	TRANSACTIONS	MODULE DESIGN	DATA DESIGN	NETWORK/ NODE DESIGN
WORKER	PERFORMANCE MEASURES	INDIVIDUAL INTERACTIONS	DETAIL STEPS	UNIT CODE	DATABASE SCHEMA	NETWORK/ NODE DESCRIPTION

Fig 1: Zachman framework on Information System Architecture

Upper Layers: Harris's security requirements are integrated by the customer, owner, and designer layer, which respectively defines the end user scope, ownership, and functionality of the system. As stated by Henning (1996), after the implementation of the first three layers of the Zachman framework, the system information flow and data structure can be visualised for Harris security engineers. Extra security-related information is added to the IDEF0 model, which is a modelling language that provides a graphical illustration of a scope or system (Kermanshachi et al., 2019). In this context, it is a prevalent model to describe the workings of each cell. According to Figure 2, the additional details support the security engineer with a clear image of the system's possible security issues. For instance, if input is identified from a specific source, the classification and owner of the source will also be validated. The potential downgrade attack can be prevented through the verification of inputs, outputs, and mechanisms classifications (Henning, 1996).

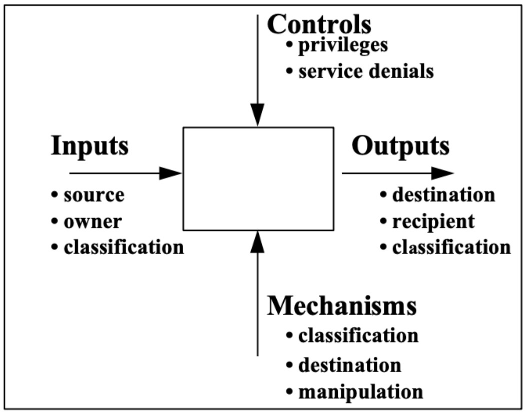


Fig 2: IDEF0 Model with Additional Security Relevant Information

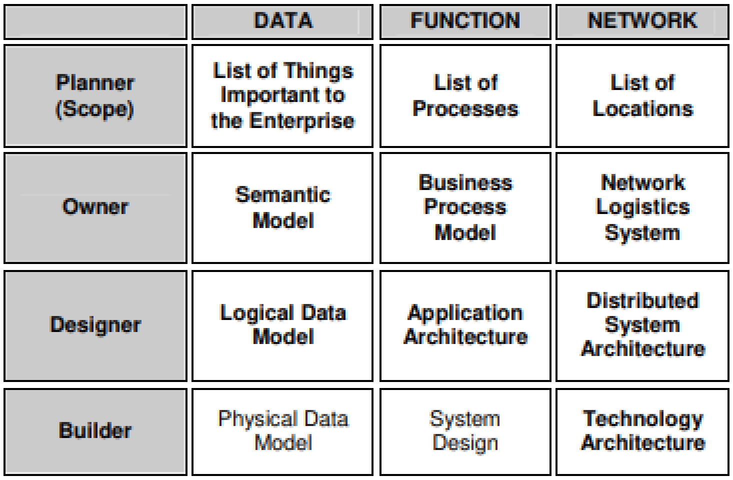
Lower Model Layers: The builder and worker layer in Harris's security policy modelling is beneficial to the security accreditation assistance (Henning, 1996). The application of these layers establishes requirement traceability to the deployment of security mechanisms, which audits the file retrieval and enhances the data access control, especially for Harris's mission plans. With the enhancement of security requirement visibility, it is easier to create system security testing strategies and guarantee the complete inclusion of requirements.

Additional Term: The case suggests that due to the complexity of merging Harris's security requirements and system architecture, the static templates from the policy guidance document (Director Central Intelligence Directive 1/16) can be incorporated with the initial Zachman framework clarification (Henning, 1996; Iyamu, 2018). This means that each operation mode and policy directive require a template to avoid redundant work and minimise the possibility of missing requirements.

4.2 Case 2 Academic Centre

Mohajerani and Moeini (2004) presents an example of using the Zachman framework to help an academic centre. Academic centres have different requirements for information security than general companies. For internal data access rights, the enterprise only needs to protect its own data with itself as the boundary. Within the company, data access is relatively open. However, in the academic centre, different internal personnel have different requirements for data resource types, and there are also many external data access requirements, such as the experimental data requirements of external personnel or remote offices of internal personnel. In addition, companies can strictly limit their Internet connections and allow employees to work in a LAN environment. However, researchers in academic centres often need to access external online libraries through the Internet to obtain bibliographies or publications.

Mohajerani and Moeini (2004) helps academic centres design cybersecurity architectures by using the Zachman framework. Using the first four rows of its matrix (Planner, Owner, Designer, Builder), it provides a four-level network security architecture attempt. And using the first three columns of the Zachman matrix (data, function, network) to examine which assets are controlled by the organisation, how they are used, and their specific location in the database.



	DATA	FUNCTION	NETWORK
Planner (Scope)	List of Things Important to the Enterprise	List of Processes	List of Locations
Owner	Semantic Model	Business Process Model	Network Logistics System
Designer	Logical Data Model	Application Architecture	Distributed System Architecture
Builder	Physical Data Model	System Design	Technology Architecture

Fig 3: The first four rows and three columns of the Zachman frame

Planner's View: First define the important content for the academic centre, such as staff and student information, experimental data, etc. Important processes such as research and teaching are then defined. Finally, define the specific geographical location of the academic centre and consider whether there are branch campuses.

Owner's View: Analysing people's behaviour and information (business process) in the academic centre, it is considered that three functional servers are needed: public service area (exchange with external information), experimental server (experimental data and self-opening software), and Trusted servers (secrets kept). In order to solve the problems of external access and data viruses, the boundary design (network logistics system) of the three servers is shown in Figure 4.

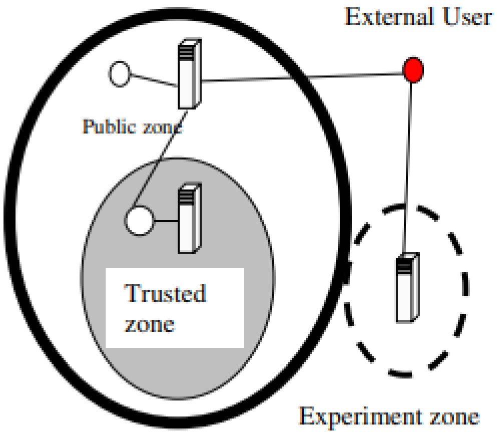


Fig 4: Academic Centre Network Layer in Owner's View

Designer's View: Introduce more specific protection network mechanisms (application architecture), such as firewalls and intrusion detection systems IDS. Clearer positioning of servers (logic model, distributed systems), e.g., separation of public service areas and trusted servers to protect confidential data as the figure shows.

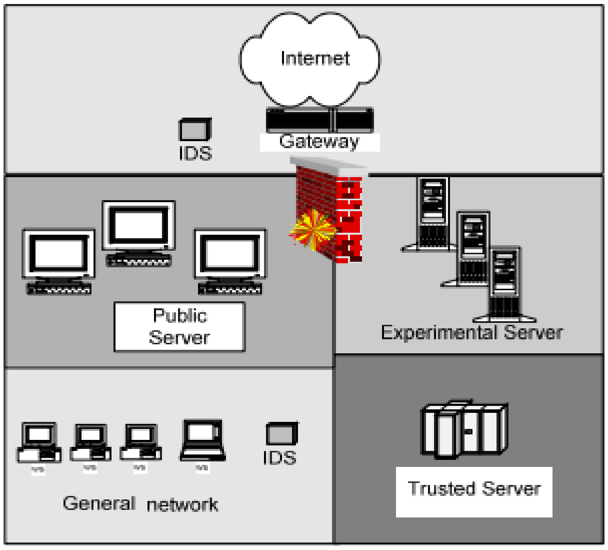


Fig 5: Academic Centre Network Layer in Designer's View

Builder's View: A more practical application view (technical architecture) was established, and suitable hardware and software on the market were used to meet the data security requirements of the academic centre.

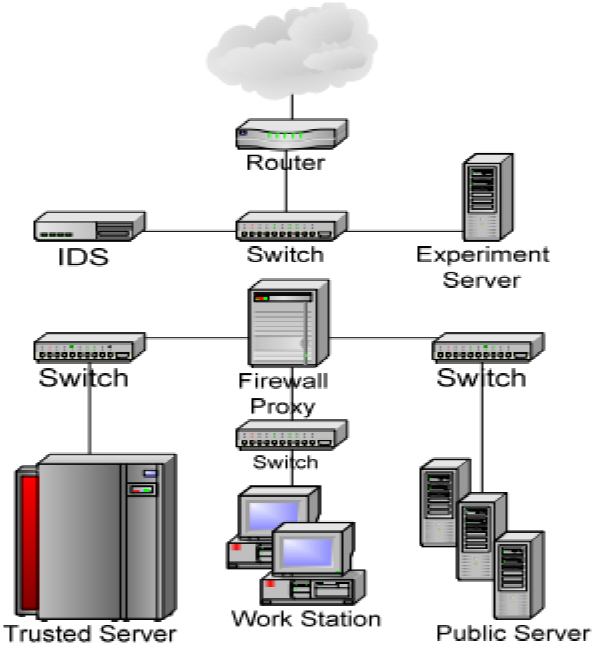


Fig 6: Academic Centre Network Layer in Builder's View

4.3 Case 3 Banking Industry

The influence of developments in information technology has spread to many sectors, including the banking industry. Case study 3 focuses on developing an EA for the banking industry using the ADM stages of the TOGAF framework, including architecture vision, business architecture, information systems architecture, technology architecture, opportunities and solution and implementation governance (Saputra & Rahmania, 2022). One of the most critical problems for banks is data security, and the TOGAF framework can be used to develop data security and management solutions in each stage related to the characteristics of the bank business. The way of improving data security with the TOGAF framework will be addressed in four phases: application architecture, information architecture, technology architecture and implementation governance.

Application architecture: This phase describes how to build the application architecture of bank systems based on the business vision. The application architecture is to deploy systems consisting of the application and the relationship for the vital process in business (Conexiam, 2023). The security, support and monitoring of system data are considered in Case Study 3 due to the importance and specificity of banking information. In the application architecture, banks develop data security monitoring that helps to improve data security and detect cyber-attacks or intrusions into the banking industry's data centre devices.

Information architecture: This phase maintains the structure of physical and logical data assets and other data structures (Conexiam, 2023). Maintaining and managing the information architecture of the database in a banking system is essential. Banks in Case Study 3 not only organise the data by groups and design the information architecture based on the relationships between business processes, but also develop tools to monitor the data and network security.

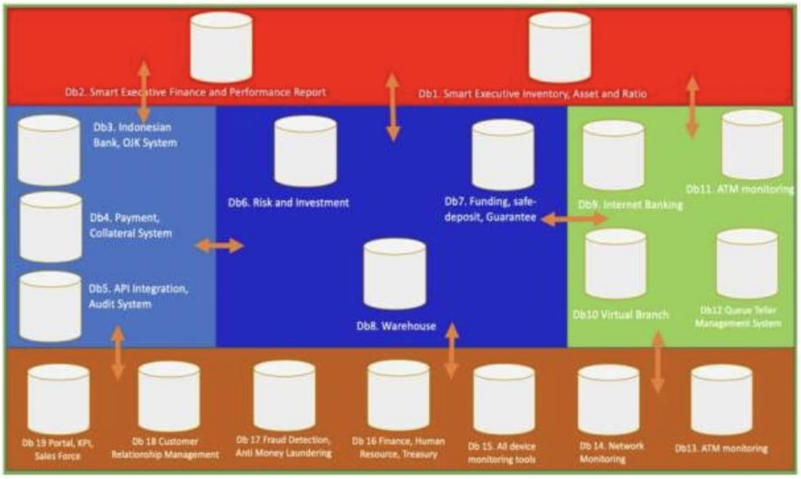

Db2. Smart Executive Finance and Performance Report
Db1. Smart Executive Inventory, Asset and Ratio
Db3. Indonesian Bank, OJK System
Db4. Payment, Collateral System
Db5. API Integration, Audit System
Db6. Risk and Investment
Db7. Funding, safe-deposit, Guarantee
Db8. Warehouse
Db9. Internet Banking
Db11. ATM monitoring
Db10 Virtual Branch
Db12 Queue Teller Management System
Db 19 Portal, KPI, Sales Force
Db 18 Customer Relationship Management
Db 17 Fraud Detection, Anti Money Laundering
Db 16 Finance, Human Resource, Treasury
Db 15. All device monitoring tools
Db 14. Network Monitoring
Db13. ATM monitoring

Fig 7: Information Architecture

Technology architecture: The bank uses a cloud computing technology architecture where the central server is not placed in a data centre room. Banks do not need to worry about data leakage and loss since technology architecture will secure networks and data, reducing the risk of data leakage if banks use additional intrusion detection systems (IDS) and intrusion prevention systems (IPS).

Implementation governance: The implementation governance phase in the TOGAF framework focuses on modifications and additions to facilities, particularly to enhance network and system security. Therefore, banks can improve their technical practices to ensure that their security measures are not limited to any particular data set or system structure.

5. Analysis

5.1 Case Comparative Analysis

Based on the examination of the three scenarios, it becomes clear that the way the Zachman framework or TOGAF is implemented depends on the feature requirements of each organisation. From Case 1 and Case 2, the Zachman framework offers a structured and holistic approach to reengineering the architecture of information systems, identifying the elements of the business that are essential to the development and management of its information systems. The Zachman framework can be used to create a cybersecurity architecture or model that supports organisations with an accurate understanding of security concerns and needs. Depending on various organisations' circumstances, the Zachman framework's matrix can be derived and widely used (Sousa et al., 2007).

In Case 1, Harris Corporation has divided the Zachman framework into two layers. The split two layers, with different perspectives based on different focuses, improve data traceability across security requirements. And in Case 2, a secure architecture for data asset access was developed based on the demands of the academic centre using the Zachman matrix with four rows and three columns rather than the entire matrix. While in Case 3, the TOGAF reorganised, directed, and developed the EA for data asset management. With outputs to safeguard data security integrated into the four architectures, the bank's system data security controls were maximised through a coherent organisational design.

However, these three cases imply that constructing a data security architecture could not solely depend on one enterprise architecture framework. The execution of an enterprise architecture framework may cooperate with other software, models, and data visualisation techniques (Rezaei & Shams, 2008). In Case 1 and Case 2, the Zachman framework has collaborated with middleware applications, IDEF models, and Venn diagrams to visualise structure development and outputs of data control security from each cell, integrating the framework into the enterprise data security system requirements. In Case 3, banking data security architecture is reconfigured through a business model canvas to outline the requirements of information systems, which helps build a data architecture for the design of TOGAF information architecture.

5.2 Overall Analysis of EA

Previous analysis showcases that applying an EA Framework can improve an organisation's cybersecurity resilience. The EA Framework provides a viable and reliable way to help organisations build their cybersecurity infrastructure and increase the resilience of their cybersecurity by strengthening their ability to respond rapidly to threats. Since a single EA Framework has the potential to be restrictive, more than one EA Framework can be used (See Appendix A) in combination or in association with other models or tools when faced with complex situations.

Firstly, the value of EA Frameworks is that they enable organisations to take a holistic view of cybersecurity, while considering elements other than technology, such as organisational structure, business processes, and people (Jalaliniya & Fakhredin, 2011). EA Frameworks play a role in data management as a governance tool that assists organisations in defining security requirements, enabling control over data structures, and visualising them. This allows the IT security department in an organisation to better regulate exposure to sensitive and private information and prevent unauthorised access. In the meantime, EA assists in identifying vulnerabilities and designing solutions, such as implementing new security protocols or upgrading IT systems (Buschle, 2014). The EA Framework helps organisations ensure that data control objectives are aligned with organisational goals and strategies, contributing to a high-level perspective of security (Mees, 2017).

Another benefit of adopting EA Frameworks is that they enable a reduction in complexity by removing duplication and redundancy effectively, increasing organisations' interoperability and agility in terms of the cybersecurity management systems. This advantage allows organisations to master the complex cybersecurity environment and business climate, maintaining a high degree of flexibility in the investment of the organisation's IT asset portfolios and business operations, and reacting rapidly to risks or opportunities. According to a recent survey by Bizzdesign, organisations with a higher level of EA maturity are more likely to have agility, which was particularly apparent during the COVID-19 pandemic of the past few years (White, 2022). Having a solid EA framework not only improves the agility of internal security systems, but also better responds to a complex and rapidly changing external environment, allowing organisations to be well-positioned both to face cybersecurity threats and to deal with a volatile external landscape (White, 2022).

Since the EA Framework establishes a consistent cross-departmental IT infrastructure for organisations, including interfaces, patterns, protocols and so on, this assists organisations in achieving standardisation and simplicity (Bossert et al., 2015). It avoids compatibility issues caused by interface problems and integration complications to a certain degree, preventing security breaches, lowering information security risks, and ensuring the interoperability of an organisation's portfolio of IT assets.

In addition, the successful establishment of cybersecurity processes is not entirely dependent on the assistance of EA Frameworks and the governance of the organisation's management. More importantly, the organisation needs to ensure transparency throughout the process to enable all departments within the organisation to have a comprehensive perspective on the IT architecture. Such transparency ensures greater open coordination between departments, preventing the occurrence of information silos and improving alignment between IT and business goals, thus facilitating the organisation's evaluation of technology purchases and other critical decision-making. With EA frameworks aligning across the organisation and sound investment in IT solutions, organisations will be able to address cybersecurity issues by achieving better capabilities and resiliency.

To sum up, although EA frameworks have the potential to be valuable in governing organisations' data security challenges by assisting them in conducting a comprehensive review of data security controls and enhancing communication and collaboration within the organisation, it is notable that EA is not a complete solution in nature. The EA framework provides a high-level structured view and general-purpose guidance, but it lacks standardised implementation details, and cannot provide customised solutions for organisations. or reveal unexpected events for them. Therefore, the EA Framework is unable to offer effective and complete assurance for an organisation's cybersecurity infrastructure on its own. Organisations are required to consider integrating the EA framework with other more specific tools, models, and standards of practice, while simultaneously promoting employee security awareness through training and organisational culture to achieve stronger cybersecurity resilience.

6. Limitations

Although our paper analyses and summarises the enhancement of EA in terms of cybersecurity resilience and discusses EA to enhance enterprise security resilience as comprehensively as possible, our paper still has some inevitable limitations:

1. The case studies analysed in this paper focus on specific industry and organisational contexts, which means that our results may not be generalisable.
2. Due to space constraints, only a limited number of cases are analysed and studied in this paper, which results in an insufficient number of cases in our sample. Also, our cases lack valid quantitative data to support the conclusion of the effectiveness of the EA framework in addressing cybersecurity challenges.
3. In addition, some emerging EA frameworks and new types of cyber-attacks are not discussed, which also creates some limitations.

We urge future research on this topic to work on breaking these limitations, including the use of more diverse case studies, collecting empirical data, and examining the effectiveness of the EA framework in a dynamic cybersecurity environment.

7. Conclusion

In conclusion, this paper has sufficiently explored how organisations can effectively apply EA frameworks, primarily Zachman and TOGAF, to enhance their cybersecurity resilience through analysing and reviewing enterprise case studies. Organisations need to seriously consider the application of EA frameworks when developing their own cybersecurity strategies, which can help them achieve better coordination and consistency in conducting multiple strategic goals such as effective enterprise management, secure data access, and rational resource allocation to enhance their cybersecurity resilience.

Furthermore, this paper also highlights the limitations of the EA framework, which cannot be considered as a complete solution by itself, although there have been cases where the EA can help enterprises greatly contribute to cybersecurity resilience. The EA framework generally lacks specific guidance for security implementation, even though Bejarano et al. (2021) have attempted to propose new EA frameworks for cybersecurity aspects of the enterprise. Enterprises in building their own cybersecurity strategies still need to consider other factors, such as the adoption and support of emerging technologies, to address cybersecurity in dynamic environments.

8. References

Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security*, 86, 402–418. https://doi.org/10.1016/j.cose.2019.07.001

Alghamdi, B., Potter, L. E., & Drew, S. (2021). Validation of architectural requirements for tackling cloud computing barriers: cloud provider perspective. Procedia Computer Science, 181, 477-486.

Al-Turkistani, H. F., Aldobaian, S., & Latif, R. (2021). Enterprise Architecture Frameworks Assessment: Capabilities, Cyber Security and Resiliency Review. *2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA)*, 79–84. https://doi.org/10.1109/CAIDA51941.2021.9425343

Bejarano, M. H., Rodríguez, R. J., & Merseguer, J. (2021, June 1). A Vision for Improving Business Continuity through Cyber-resilience Mechanisms and Frameworks. IEEE Xplore. https://doi.org/10.23919/CISTI52073.2021.9476324

Bhatia, K., Pandey, S. K., & Singh, V. K. (2023). Enterprise Architecture Frameworks for Security Establishment. *2023 International Conference on Artificial Intelligence and Smart Communication (AISC)*, 11–17. https://doi.org/10.1109/AISC56616.2023.10085439

Boehm, J., Dias, D., Lewis, C., Li, K., & Wallance, D. (2022). Cybersecurity trends: Looking over the horizon. *McKinsey & Company. March*, 10.

Bossert,O., Richter, W., & Weinberg, A. (2015, March 1). Protecting the enterprise with cybersecure IT architecture. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/protecting-the-enterprise-with-cybersecure-it-architecture

Buschle, M. (2014). Tool Support for Enterprise Architecture Analysis: with application in cyber security. *Doctoral dissertation, KTH Royal Institute of Technology*.

Chmielecki, T., Chołda, P., Pacyna, P., Potrawka, P., Rapacz, N., Stankiewicz, R., & Wydrych, P. (2014). Enterprise-oriented Cybersecurity Management. Proceedings of the 2014 *Federated Conference on Computer Science and Information Systems*. https://doi.org/10.15439/2014f38

Conklin, W. A., Shoemaker, D., & Kohnke, A. (2017). Cyber resilience: Rethinking cybersecurity strategy to build a cyber resilient architecture. Reading: Academic Conferences International Limited. https://www.proquest.com/conference-papers-proceedings/cyber-resilience-rethinking-cybersecurity/docview/1897660614/se-2

Conexiam. (2023). Enterprise architecture domains. Retrieved from https://conexiam.com/enterprise-architecture-domains/

Ekstedt, M. & Sommestad, T. (2009). Enterprise architecture models for cyber security analysis. https://ieeexplore.ieee.org/abstract/document/4840267/authors#authors

Gillis, A. S. (2023). Enterprise architecture framework. https://www.techtarget.com/searchapparchitecture/definition/enterprise-architecture-framework

Haughey, C. J. (2020, November 19). Cybersecurity Framework: How To Create A Resilience Strategy. *Security Intelligence*. https://securityintelligence.com/articles/how-to-create-a-cybersecurity-framework/

Henning, R. R. (1996). Use of the Zachman Architecture for Security Engineering - NIST. https://csrc.nist.gov/csrc/media/publications/conference-paper/1996/10/22/proceedings-of-the-19th-nissc-1996/documents/paper044/baltppr.pdf

Iyamu, T. (2018). Implementation of the enterprise architecture through the zachman framework. *Journal of Systems and Information Technology*, 20(1), 2–18. https://doi.org/10.1108/jsit-06-2017-0047

Jalaliniya, S., & Fakhredin, F. (2011). Enterprise Architecture and Security Architecture Development. https://www.semanticscholar.org/paper/Enterprise-Architecture-and-Security-Architecture-Jalaliniya-Fakhredin/3d4b9a98e053aa334e2523276e01cc2c567fce5c

Kermanshachi, S., Safapour, E., Anderson, S., Goodrum, P., Taylor, T., & Sadatsafavi, H. (2019). *Development of multi-level scoping process framework for transportation infrastructure projects using IDEF modeling technique*. ResearchGate. https://www.researchgate.net/profile/Sharareh-Kermanshachi/publication/328978892_Development_of_Multi-Level_Scoping_Process_Framework_for_Transportation_Infrastructure_Projects_Using_IDEF_Modeling_Technique/links/5c004c1492851c63cab048c7/Development-of-Multi-Level-Scoping-Process-Framework-for-Transportation-Infrastructure-Projects-Using-IDEF-Modeling-Technique.pdf

KnowledgeHut. (2023, April 21). TOGAF in Data Architectural Way. https://www.knowledgehut.com/blog/it-service-management/togaf-data-architectural-way

Koenen, S. (2015). Assessing The Level of Security of An Organization by Analyzing The Enterprise Architecture : A Methodology. http://essay.utwente.nl/66920/1/Koenen_MA_EEMCS.pdf

Larno, S., Seppänen, V., & Nurmi, J. (2019). Method framework for developing enterprise architecture security principles. *Complex Systems Informatics and Modeling Quarterly*, 117(20).

Mees, W. (2017). Security by design in an enterprise architecture framework. Royal Military Academy, Department CISS, Renaissancelaan, 30, 1000.

Mohajerani, M., & Moeini, A. L. I. (2004). Using enterprise architecture framework to design network security architecture. *WSEAS Transactions on Communications*, 3(2), 688-693.

Monino, J.-L. (2020). Data Control Major Challenge for the Digital Society. John Wiley & Sons, Incorporated.

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., &amp; Masood Siddiqui, A. (2021). Real-time analytics, incident response process agility and Enterprise Cybersecurity Performance: A contingent resource-based analysis. International Journal of Information Management, 59, 102334. https://doi.org/10.1016/j.ijinfomgt.2021.102334

Oda, S. M., Fu, H., & Zhu, Y. (2009). Enterprise information security architecture A review of frameworks, methodology, and case studies. 2009 2nd IEEE International Conference on Computer Science and Information Technology. https://doi.org/10.1109/iccsit.2009.5234695

Ovaledge. (2021, September 29). Data Access Management Basics & Implementation Strategy. https://www.ovaledge.com/blog/data-access-management-basics-implementation-strategy

Ramadan, A. B. & Hefnawi, M. (2007). A NETWORK SECURITY ARCHITECTURE USING THE ZACHMAN FRAMEWORK. https://www.researchgate.net/profile/Abou-Bakr-Ramadan/publication/226076238_A_Network_Security_Architecture_Using_The_Zachman_Framework/links/5a172d9aaca272df0808aa8a/A-Network-Security-Architecture-Using-The-Zachman-Framework.pdf

Rezaie, M., Mirzahosein, Z. & Rasouli, H. (2022). Developing a Digital Transformation Architecture Framework: A Business Intelligence Approach. https://ieeexplore.ieee.org/abstract/document/10054019

Rezaei, R., & Shams, F. (2008). A methodology to create data architecture in Zachman Framework. ResearchGate. https://www.researchgate.net/publication/253934154_A_Methodology_to_Create_Data_Architecture_in_Zachman_Framework

Sessions, R. (2007). Comparison of the top four enterprise architecture methodologies. http://rogersessions.com/images/PapersAndBooks/TopFourEAMethodologies.pdf

Shepherd, J. (2011). *How to get started with a pace-layered application strategy*. Gartner. https://www.gartner.com/en/documents/1607414

Sousa, P., Pereira, C., Vendeirinho, R., Caetano, A., & Tribolet, J. (2007). Applying the Zachman framework dimensions to support business process modeling. *Digital Enterprise Technology*, 359–366. https://doi.org/10.1007/978-0-387-49864-5_42

Saputra, F. B., & Rahmania, E. (2022). Banking Information System Study Through Enterprise Architecture TOGAF. *NEWTON: Networking and Information Technology*, *2*(1), Article 1. https://doi.org/10.32764/newton.v2i1.2597

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, pp-pp. https://doi.org/10.17705/1CAIS.02810

Tong, Y., Zhang, J., Xu, M.-D., & Qin, T. (2015). Network Security Monitoring and Defense System Framework Design Using Mobile Agents Based on DoDAF. *2015 International Conference on Computer Science and Applicatio*ns (CSA), 366–370. https://doi.org/10.1109/CSA.2015.73

White, S.K. (2022, November 23). What is enterprise architecture? A framework for transformation. https://www.cio.com/article/222421/what-is-enterprise-architecture-a-framework-for-transformation.html

Zachman, J. A. (1997). Enterprise architecture: The issue of the century. *Database Programming and Design*, 10(3), 44-53. https://cioindex.com/wp-content/uploads/nm/articlefiles/63503-EAIssueForTheCenturyZachman.pdf

Zachman, J.A. (2003). The zachman framework for enterprise architecture: Primer for Enterprise Engineering and Manufacturing . *Zachman International*. https://www.dragon1.com/downloads/ZachmanBookRFIextract.pdf

9. Appendices

Appendix A - the importance of EA framework in enterprise network security, using the data control system as an example.

Framework	**Role and Impact on Data Control Management**	**Data Access Management**	**Data Monitoring Management**
Zachman	- It provides a method for creating data architecture to consider the process of creating data architecture designer view, data architecture equivalence and the	**Yes** - It can determine who is allowed to access each data group and where these people are located	**No** - It doesn't provide specific guidance on data monitoring process.

	function through adapting entities with processes (Rezaei & Shams, 2008). - It has not considered security concerns explicitly, but some security architecture frameworks have been developed based on Zachman Framework (Jalaliniya & Fakhredin, 2011).	(Jalaliniya & Fakhredin, 2011).	
TOGAF	- It considers data security as secondary action that is combined with the data architecture designed (Jalaliniya & Fakhredin, 2011). - But no methodology mentioned to develop security architecture (Jalaliniya & Fakhredin, 2011).	**Yes** - It has considered the data security diagram as a part of data architecture that shows each actor can access which data (Jalaliniya & Fakhredin, 2011). - Data architecture describes how enterprise data is stored, managed and accessed.	**Partial** - Data aspects that can be monitored are mentioned in the data architecture.
DoDAF	- The security-related data in DoDAF are mentioned to support procedural, communications security (COMSEC), and Information Security (INFOSEC) concerns (Jalaliniya & Fakhredin, 2011). - Play a role in improving data control management through a data exchange matrix that describes the relationship between data elements (Tong et al., 2015).	**Partial** - DoDAF emphasises security elements and their relationships but lacks guidance on the development process. - Help improve the design of data access.	**Partial** - Help improve the design of data monitoring.

Gartner’s Pace-Layer Framework	- Support and manage the organisation's critical master data (Shepherd, 2011).	**No** - No guidance was provided on the data access aspect.	**No** - No provision of methods for data monitoring.
Federal Enterprise Architecture Framework (FEAF)	- Includes data standards used for upgrading from current to target architecture (Jalaliniya & Fakhredin, 2011).	**Yes** - Having a security principle for protecting data from unauthorised access (Jalaliniya & Fakhredin, 2011).	**Yes** - A software tool used to assess different phases of security architecture (Jalaliniya & Fakhredin, 2011).