Security Architecture Framework for Enterprises (SAFE)

Vender Yanto Salim
University of Melbourne
vender.salim@gmail.com

Siti Ulfah Lukman
University of Melbourne
ulfahlukman@gmail.com

Garda Yaumil Akhir
University of Melbourne
garda.akhir@gmail.com

Zyan Tharra Ardina
University of Melbourne
zyan.tharra@gmail.com

Bramantyo Adi Nugroho
University of Melbourne
bramantyo.pn@gmail.com

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

Abstract

As organizations face increasing cybersecurity risks due to accelerated digitalization, the adoption of the International Organization for Standardization (ISO) 27001 standard for Information Security Management has become widespread. However, through a literature review, this report identifies four key challenges persisting in implementing this standard, including alignment with business goals, resource constraints, poor organizational change management, and the complexity of the IT landscape. Further research indicates that Enterprise Architecture (EA), particularly the TOGAF®[1] framework, can effectively address these challenges and integrate ISO 27001 standards. Through a strategic and comprehensive approach, EA aligns business objectives with IT systems and infrastructure, enabling effective management, governance, and decision-making. While adopting EA addresses these challenges at the conceptual level, practical implementation requires equipping the EA framework with a security architecture layer to embed security considerations throughout the architecture development process. Therefore, the paper concludes by introducing the Security Architecture Framework for Enterprise (SAFE) as an integration framework for ISO 27001 and TOGAF®, SAFE offers actionable insights and solutions to integrate security controls within EA, facilitating the effective implementation of cybersecurity initiatives at the enterprise level.

Keywords:
Cybersecurity; Information Security; ISO 27001; Enterprise Architecture; TOGAF®.

1. Introduction

The accelerated digitalization and advancement of information technology exposes every organization to cyber-attacks. Every organization needs to take various steps to achieve its security objectives (Ganji et al., 2019). According to a recent study by the Identity Theft Resource Center (2024), the number of data breaches in 2023 increased by over 78% compared to 2022, indicating a significant rise in cybersecurity threats.

To address these challenges, organizations have developed various approaches, including the adoption of security standards, models, and frameworks (Ganji et al., 2019). Despite the absence of solid evidence for absolute security, some popular and well-known approaches, such as the ISO 27001 standard, have been widely adopted globally. Table 1 represents the growth statistics of the ISO 27001 standard from 2021 to 2022, showing a global increase of 21%.

[1] TOGAF is a registered trademark of The Open Group.

Table 1. Growth of ISO Standard adoption from 2021 to 2022 (ISO, 2022)

	Number certificates from providers took part in 2021 and 2022	variation total	variation in %
ISO 9001:2015	1024674	126524	12
ISO 14001:2015	485054	85725	21
ISO 45001:2018	367182	83076	29
ISO/IEC 27001:2013	67326	11549	21
ISO 50001:2011&2018	26625	6611	33

ISO 27001 is an international standard that provides guidelines for establishing, implementing, maintaining, and improving an information security management system (ISMS). This standard is applicable to most organizations regardless of their size, sector, activity, or core business type (ISO, 2022).

While implementing security standards is crucial, organizations still face challenges. According to a study by Alshitri and Abanumy (2014), resource constraints and budgetary limitations result in low implementation of ISO 27001 in some countries. Additionally, organizations find it difficult to align the security standard with their business objectives, often viewing it merely as a technical requirement rather than an integral part of their broader business objectives (Everett, 2011).

To address these challenges, we examined the EA approach as a potential solution, as it provides organizations with a better understanding of how information security could benefit their business and operations (Andrews et al., 2014). The architectural approach enhances information security by integrating security into every aspect of the design of information systems (Loft et al., 2019). Thus, information security becomes more manageable and aligns with the organization's business objectives. A recent study shows that TOGAF® frameworks are considered significantly superior compared to other common architectural frameworks, such as the Zachman Framework™, Gartner Framework, and Federal Enterprise Architecture (Kotusev, 2018).

However, integrating information security and EA poses a challenge, as information security has traditionally been considered a separate discipline, detached from business processes and EA (The Open Group, 2018). Therefore, this study is conducted based on the following research questions that discuss the information security implementation challenges, how EA can address these challenges, and the integration of ISO 27001 standards and TOGAF® frameworks.

Research Question:

RQ1: How can EA become a potential solution to address the challenges and enhance the effectiveness of implementing information security programs?

RQ2: How can information security requirements be embedded and integrated into EA?

The remainder of this paper is organized as follows: we conduct a literature review to identify key challenges in implementing ISO 27001, followed by addressing these obstacles using TOGAF®.

After that, we present our proposed SAFE framework for integrating the security standard into the EA framework through the mapping of ISO 27001 requirements into TOGAF®. We then discuss limitations and opportunities for future research and conclude in the final section.

2. Literature Review

2.1. ISO27001 Implementation Challenges

While organizations increasingly recognize the importance of adopting ISO 27001 to enhance their information security posture, build trust with stakeholders, and ensure compliance with regulatory requirements, several challenges persist in its implementation. To identify these challenges, we conducted a literature review using the following approach.

The concept of Enterprise Information Security Architecture gained recognition around 2005 (Shariati et al., 2011). Therefore, we conducted a search spanning the last twenty years (2005 to 2024) using keywords like ISO 27001, Information Security Management Systems (ISMS), Cybersecurity, and implementation or adoption challenges in the Compendex, Inspec, and IEEE databases (engineering management and business databases). Non-English articles and those with zero citations were excluded. All papers were selected and analyzed by team members who are practitioners in ISO 27001 standard implementation, resulting in the following 12 highly relevant articles highlighting the complexities of ISO 27001 implementation.

Kitsios et al. (2023) identified that implementing controls and conducting risk assessments complicate internal processes, impacting change management. Moreover, the requirement for ISO 27001 compliance adds to the significance of these challenges within an organization's lifecycle. Mirtsch et al. (2020) described low adoption rates due to high costs, paperwork burdens, limited integration with existing business processes, and difficulty quantifying benefits. Neubauer et al. (2008) stressed the cost and lack of evidence for positive cost/benefit ratios as barriers to adoption.

Additionally, Hagen et al. (2008) found technical measures prioritized over awareness creation despite the latter's effectiveness. Broderick (2006) argued that ISMS implementation requires executive management drive, not just reliance on security departments. Gillies (2011) claimed cultural change and senior management support as key implementation barriers.

Moreover, Anttila et al. (2012) highlighted the risk of ISO 27001 projects being perceived solely as IT initiatives rather than strategic organizational endeavors. Challenges in identifying assets and associated risks, especially in complex environments like cloud, are noted by Beckers et al. (2011), Haris (2018), and Velasco et al. (2018). AbuSaad et al. (2011) emphasized budget constraints, negative employee attitudes, lack of top management involvement, and incompatibility with existing policies and procedures as further challenges. Soliman and Ojalainen (2023) concluded that the challenge of reconciling security measures with convenience required a cultural shift within organizations.

Analysis of the relevant literature above reveals four key obstacles to ISO 27001 adoption in enterprises:

1. **Lack of Alignment with Business Goals:** Enterprises often struggle to align ISO 27001 implementation with their overarching business objectives. Without clear communication

and understanding of how information security contributes to these goals, senior management and stakeholders may resist or deprioritize compliance efforts.

2. **Resource Constraints and Budgetary Limitations:** Implementing ISO 27001 requires significant investment in time and resources. Many enterprises, regardless of size, may find it challenging to allocate sufficient funds and manpower for compliance, leading to incomplete implementation or delays.
3. **Poor Organizational Change Management:** ISO 27001 implementation necessitates changes in processes, technology, and organizational culture. Without effective change management practices, employee resistance can hinder adoption and integration by perceiving new security measures as burdensome.
4. **Complexity of IT Landscape:** Enterprises operate in complex IT environments with a mix of legacy systems, cloud services, and third-party applications. Securing this landscape in compliance with ISO 27001 standards, especially in the absence of asset catalogs, poses significant challenges in identifying assets, managing risks, and ensuring consistency in security measures.

Table 2 maps the challenges identified in the literature into four key groups.

Table 2. Key challenges mapping with the challenges presented in the 12 literatures

Literatures	Lack of Alignment with Business Goals	Resource Constraints and Budgetary Limitations	Poor Organizational Change Management	Complexity of IT Landscape
Kitsios et al., 2023			X	
Mirtsch et al., 2020	X	X		
Neubauer et al., 2008	X	X		
Hagen et al., 2008			X	
Broderick, 2006			X	
Gillies, 2011			X	
Anttila et al., 2012	X			
Beckers et al., 2011				X
Haris, 2018				X
Velasco et al., 2018				X
AbuSaad et al., 2011	X	X	X	
Soliman and Ojalainen, 2023			X	

2.2. Addressing Key Challenges by TOGAF®

EA could play a strategic and comprehensive role in ensuring the successful implementation of the ISO 27001 program at the enterprise level. It provides a holistic approach to integrating ISO 27001 into the enterprise by ensuring that technology, business goals, processes, information flows,

and people of the organization are equally considered (Dzazali et al., 2009; Soomro et al., 2016), addressing the four key challenges as follows.

Lack of Alignment with Business Goals

Loft et al. (2019) highlighted that architectures enforce a holistic view in organizations, specifically when using TOGAF®, aligning business vision, drivers, and capability for organization-wide initiatives (see Figure 1). Security should not excessively impede business function, but business processes must consider security constraints, including legislative and regulatory requirements (Atay & Masera, 2011). TOGAF® helps organizations understand business drivers, requirements, and constraints (The Open Group®, 2018). This alignment ensures that information security program implementation is driven by business priorities, integrating security measures into business processes and decision-making (Loft et al., 2019).

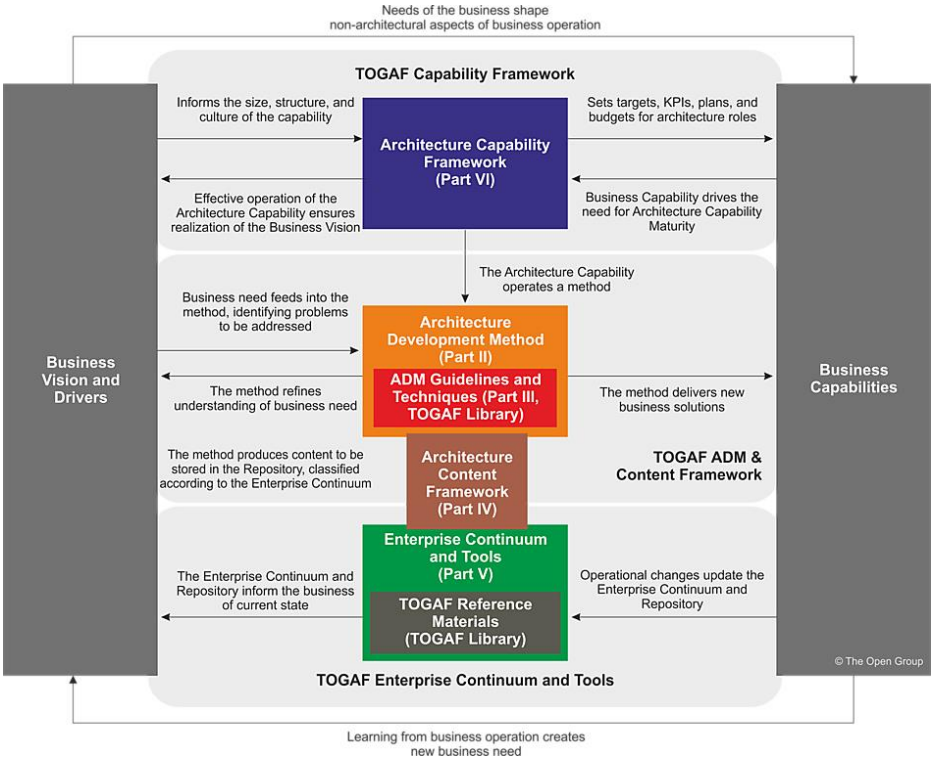

Figure 1. Structure of the TOGAF Standard (The Open Group, 2018)

Resource Constraints and Budgetary Limitations

EA enables organizations to evaluate their application and project portfolios for well-balanced IT investment decisions (Quartel et al., 2012). Specifically using TOGAF®, it aligns security initiatives with business goals to prioritize efforts strategically. TOGAF® also promotes modularization and asset reuse, reducing duplication of work and maximizing resource utilization. Additionally, stakeholder engagement throughout the development process facilitates buy-in and support, aiding budget and resource allocation. Moreover, TOGAF®'s risk management processes

prioritize resource allocation based on risk significance, and its iterative approach allows for incremental adoption, aligning with the ISO 27001 implementation scoping approach. Leveraging these aspects, organizations overcome resource constraints and budgetary limitations, ensuring successful ISO 27001 implementation while optimizing resource utilization.

Poor Organizational Change Management

EA supports change impact analysis (for planning changes) and propagation (for implementing changes) to ensure the success of organizational changes (Dam et al., 2016). Specifically, TOGAF®'s Architecture Vision and Change Management capabilities enable organizations to develop a clear vision for the desired state of security architecture at the enterprise level. By engaging stakeholders and conducting impact assessments early in the architecture development cycle, TOGAF® identifies change management requirements and develops strategies to address resistance, enhancing organizational buy-in and facilitating smoother adoption of ISO 27001 practices.

Complexity of IT Landscape

The TOGAF® Architecture Development Method (ADM) addresses IT landscape complexity in ISO 27001 projects by providing a structured approach to asset identification and management. During the ADM's Business, Information Systems, and Technology Phase, organizations identify and catalog all relevant assets and their relationships, including processes, data, software, and hardware (see Figure 2). This process ensures a clear understanding of the IT landscape, crucial for ISO 27001 implementation. Additionally, TOGAF® prioritizes assets based on their criticality to business operations and information security, allowing resource allocation to focus on protecting the most vital assets, mitigating risks, and enhancing security (The Open Group, 2018).

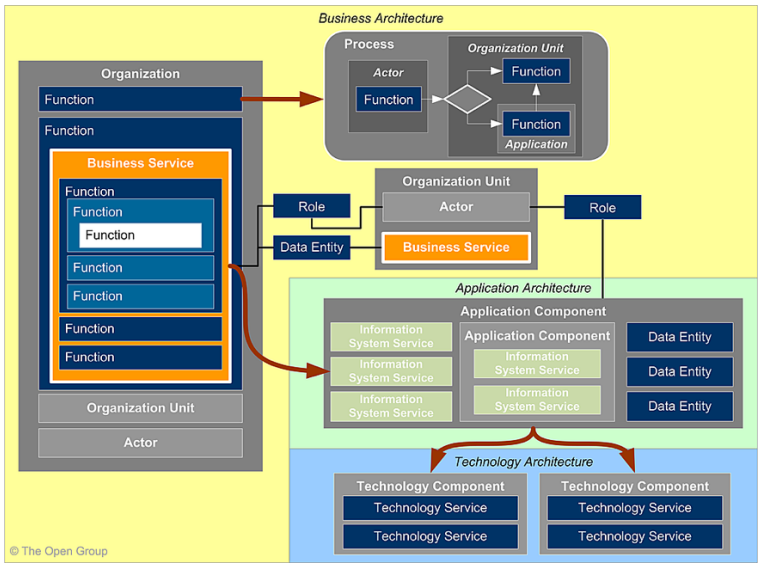

Figure 2. Core Entities and their Relationships (The Open Group, 2018)

While the conceptual justification of how TOGAF® addresses ISO 27001 implementation challenges is evident, practical guidance on integrating these frameworks and standards is crucial for organizations. Moreover, there is a need for the TOGAF® Framework to be equipped with a security architecture layer and no fixed mapping has been made to the ISO27001 standard (The Open Group, 2018). Therefore, we introduce the Security Architecture Framework for Enterprises (SAFE) for effective integration of TOGAF® and ISO 27001 in organizations in the next section.

3. Security Architecture for Enterprises (SAFE)

3.1. ISO27001 and TOGAF®

International Organization for Standardization (ISO) 27001

ISO 27001 is an international standard that defines requirements for Information Security Management Systems (ISMS). Its objective is to preserve the confidentiality, integrity, and availability of an organization's information assets. The standard assists organizations in assessing, establishing, and improving their information security systems while considering business needs and objectives. By implementing ISO 27001, organizations are expected to develop a comprehensive managerial perspective on information security, enabling them to proactively mitigate and address evolving security risks. While not a methodological framework, ISO 27001 provides a structured approach to information security management through its iterative Plan-Do-Check-Act (PDCA) cycle, allowing for continuous improvement of information security controls implementation.

This study utilizes the ISO 27001:2022 version due to its latest requirements and controls for ISMS standards. Compared to its previous 2013 version, this version includes minor updates to Clauses 4 to 10 and significant changes in Annex A. These changes involve terminology and sentence restructuring in the clauses, and a reduction in risk controls from 114 to 93 in the annex, along with the addition of 11 new security control standards to address emerging cyber threats and modern security practices (Malatji, 2023).

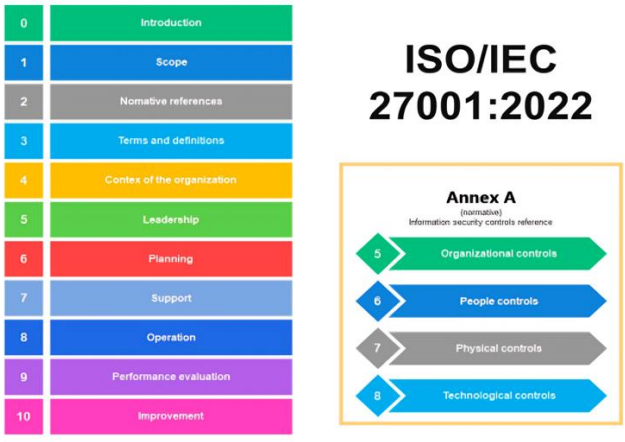

Figure 3. ISO/EIC 27001:2022 Structure (Barraza de la Paz et al., 2023)

The Open Group Architecture Framework (TOGAF®)

TOGAF® is an EA framework that offers methods, tools, and guidelines for designing, producing, and maintaining EA. Its primary objective is to standardize and maintain consistency within the architecture development process, aiming to enhance productivity and cost efficiency. One of its key strengths is scalability, making it suitable for businesses of any size. Additionally, TOGAF® is flexible, allowing adjustments based on specific needs and objectives, as well as integration with other frameworks or standards.

TOGAF® 9.2, published in 2018, is the most relevant version for this study. It provides a variety of guidance, including a guideline for integrating risk and security into TOGAF®-based architecture (The Open Group, 2018). The widespread adoption of TOGAF® 9.2 has led to the development of a community of practitioners and established training and certification initiatives, indicating the most relevant version to date.

The Architecture Development Method (ADM) within TOGAF® offers an iterative and controlled approach to realizing business goals and objectives. It is a process for architecture development across four domains: business, data, application, and technology. The ADM consists of nine phases, beginning with the Preliminary Phase and followed by eight phases iteratively implemented around requirements management. This method is intentionally generic, allowing for modifications to meet specific needs and accommodate enterprise maturity, enabling the creation of an enterprise-specific ADM (The Open Group, 2018).

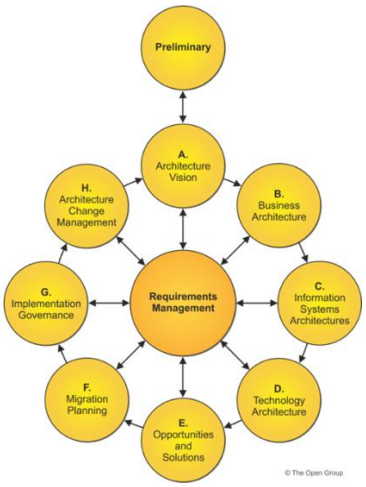

Figure 4. TOGAF® ADM (The Open Group, 2018)

3.2. ISO27001:2022 – TOGAF® 9.2 ADM Integration Approach

ISO 27001 provides a comprehensive and directive set of standards for information security management practices in organizations. In contrast, TOGAF® offers a structured yet flexible approach for EA development through the ADM. Although security is not a core

domain of architecture in the TOGAF® ADM, it allows for the integration of concepts such as risk and security (The Open Group, 2018).

Figure 5. Security as cross-cutting concern (The Open Group, 2018)

TOGAF® recognizes security as a cross-cutting concern that impacts all aspects of the EA domain (The Open Group, 2018). The security architecture is often structured outside the main architectural domain, but certain elements must be developed in coordination with the overall EA to ensure alignment. Furthermore, there is no fixed mapping of ISO 27001 security requirements to TOGAF® ADM (The Open Group, 2018), despite both frameworks being widely adopted. Thus, SAFE is introduced as guidance to incorporate ISO 27001:2022 security elements into TOGAF® ADM-based EA. ISO 27001 focuses on specifying what information security controls and processes should be in place, and TOGAF® guides practitioners to plan and design these implementations within an organization's broader context, addressing its specific needs, business objectives, and risks.

In this paper, we align TOGAF® 9.2 with ISO 27001:2022 requirements following TOGAF®'s Guidelines on Security Architecture and the ADM. We will also incorporate insights from TOGAF® Guidelines to Integrating Risk and Security and previous publications on integrating TOGAF® with other security frameworks such as SABSA. Based on this literature, we integrate ISO 27001 security requirements into each phase of the ADM's artifacts, ensuring that security is embedded throughout the EA.

The Integration is based on the following foundations:

1. **TOGAF® and ISO 27001 are fundamentally requirements-driven.** TOGAF® employs a business-focused approach, continuously validating and updating EA requirements throughout the cycle to align with business objectives. Meanwhile, ISO 27001 presents a set of information security requirements that organizations must fulfill to maintain compliance. It also emphasizes implementing specific controls and processes tailored to an organization's needs, which is critical for ensuring that security measures align with the organization's risk profile.
2. **Risk management is an integral concept in EA**, addressing threats that may arise from business operations which are influenced by processes, systems, people, and technology

(The Open Group, 2011). Both TOGAF® and ISO have similar approach in managing risks (ISO, 2022; The Open Group, 2018). Furthermore, ISO 27001 specifies controls in such areas as organizational, people, physical, and technology to mitigate security risks that is a key aspect of an organization's operational risk.

3. **TOGAF® and ISO 27001 produce artifacts during their respective processes.** ISO 27001 requires a set of documents or evidence, deemed security artifacts, to fulfill control requirements. We identify and integrate these security artifacts into each phase of the ADM to ensure that security is incorporated into the EA cycle.

Using the artifacts mapping approach (The Open Group, 2011), we perform the following method:

1. Analysis of requirements from ISO 27001 and derive the required security artifacts.
2. Map these security artifacts into the appropriate TOGAF® ADM phase. In mapping, we adhere to the following rules:
   - When an artifact appears at different architectural levels, we map it at the highest level of abstraction to maintain the focus on the enterprise level.
   - Integration is focused on the most critical elements in ISO 27001 (risk management, controls implementation, management oversight).

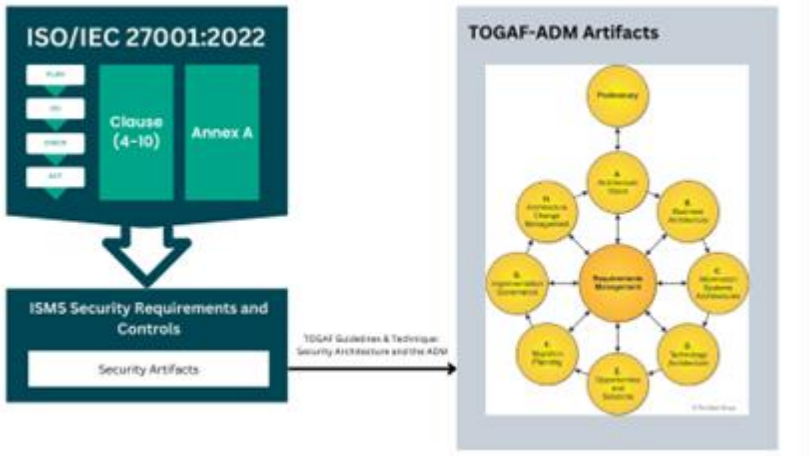

Figure 6. TOGAF® ADM-ISO 27001 Integration Approach

3.3. Integrating ISO27001:2022 Requirements with TOGAF® 9.2 ADM

ISO 27001 employs the PDCA cycle to ensure continuous improvement in managing and maintaining an ISMS. Similarly, the TOGAF® ADM shares fundamental iterative approaches to development and improvement. Figure 7 represents the mapping of the ISO 27001 PDCA cycle and the TOGAF® ADM as an integration baseline for the SAFE framework.

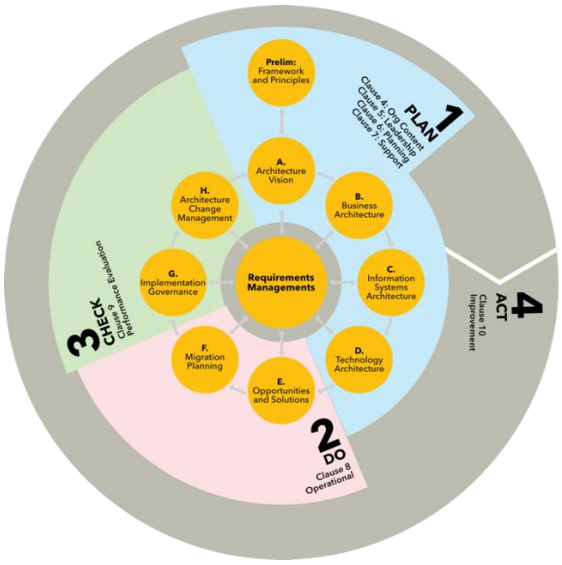

Figure 7. PDCA-Cycle and TOGAF® ADM

ISO 27001 essentially requires that organizations have the following components (The Open Group, 2018):

- **Risk Assessment**: Conducting a thorough analysis of the organization's information security risks, considering potential threats, vulnerabilities, and impacts.
- **Control Implementation**: Implementing security controls or risk mitigation strategies for risks deemed unacceptable.
- **Management Oversight**: Establishing a management process to ensure ongoing alignment of implemented information security controls with the organization's needs.

Integrating these components into the EA, we map the required ISO 27001 security artifacts into the TOGAF® ADM. These security requirements could either be outputs that need to be produced during the phase, or elements that can be integrated into existing EA artifacts.

Security policies, standards and objectives set at the enterprise level are integrated into EA requirements and become mandatory for all subsequent architecture domains (The Open Group, 2018). In the Preliminary phase, aligning with the planning activities of ISO 27001, the ISMS scope is established. Additionally, security principles and capabilities could be embedded into Architecture Principles and Capabilities to align with the EA high-level vision.

ISO 27001 clause requirements related to planning and management support—including context of the organization (clause 4), leadership (clause 5), planning (clause 6), and support (clause 7)—are integrated into the early phases of the TOGAF® ADM (Preliminary and Vision), to align security measures planning with the organization’s business strategies.

In developing current and target Business Architectures, organizations should also identify valuable assets and potential risks to them, including information security risks. Risks are assessed to identify potential threats and vulnerabilities that impact overall business operations.

Subsequently, appropriate mitigating strategies, including the implementation of security controls, are put in place to manage and reduce these risks effectively.

The security controls that consist of organizational, people, physical, and technological, are then developed and implemented during phases B, C, D, and E. During the operational phase, security aspects of the architecture must be monitored, assessed, and reported. While it usually begins following one iteration of the TOGAF® ADM, the design and integration of security measurement capabilities take place in Phases G and H (The Open Group, 2018).

This overall integration results in a Security Architecture Framework for Enterprises (SAFE), as shown in Figure 8, detailing how information security requirements should be embedded and integrated into EA, offering practical guidance for organizations to effectively implement their enterprise security initiatives and EA.

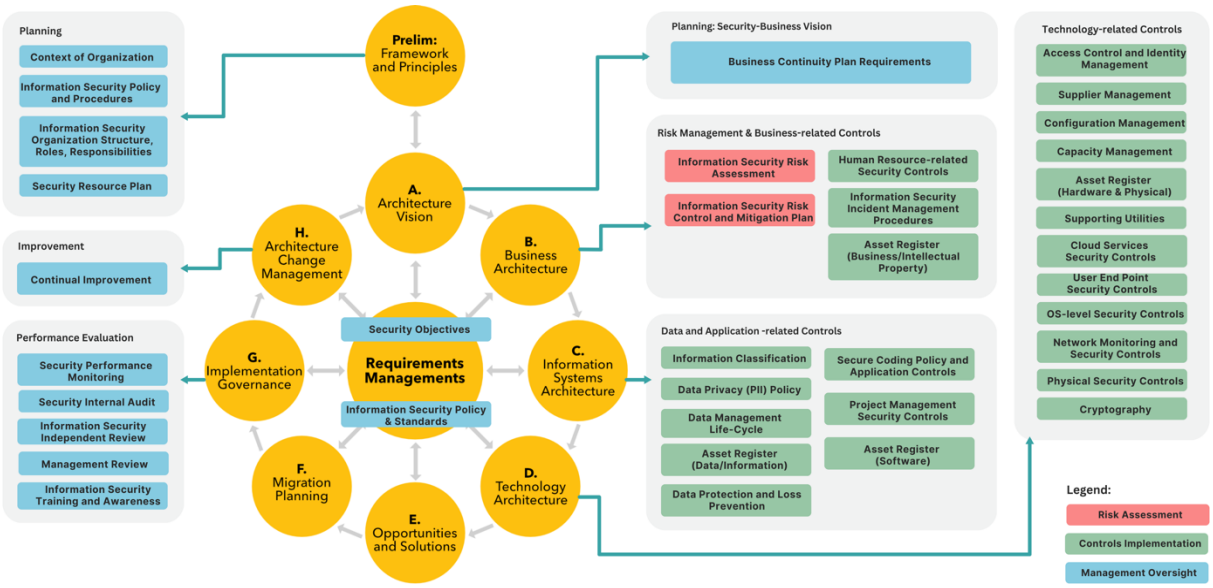

Figure 8. SAFE

The detailed mapping of ISO/IEC 27001:2022 information security requirements to the TOGAF® ADM artifacts is presented in the table below:

TOGAF® ADM Phase	**Relevant TOGAF® ADM Outputs/ Artifacts (TOGAF®, 2018)**	**TOGAF® Guidelines & Techniques: Security and ADM (TOGAF®, 2018)**	**ISO27001:2022 Requirements Mapping**	
			References	**Security Artifacts**
Requirements Management	Requirements Catalogue	The security standards and security policy are integrated into the EA requirements management process.	Clause 5.2 Policy, Clause 6.2 Information Security Objectives, Annex 5.31 Legal,	• Information Security Objectives • Information Security Policy and Procedures

TOGAF® ADM Phase	Relevant TOGAF® ADM Outputs/ Artifacts (TOGAF®, 2018)	TOGAF® Guidelines & Techniques: Security and ADM (TOGAF®, 2018)	ISO27001:2022 Requirements Mapping	
			References	Security Artifacts
			statutory, regulatory and contractual requirements	
Preliminary	Architecture Capability: • Architecture Principles • Organizational Model for EA (including scope of organization, key drivers, roles and responsibilities, budget, constraints, governance and support strategy)	• Scope the enterprise organizations impacted by the security architecture. • Define and document applicable regulatory and security policy requirements. • Define the required security capability as part of Architecture Capability. • Implement security architecture tools.	Clause 4 Context of Organization	• Context of Organization (scope of ISMS, issues, stakeholders' needs and expectations)
			Clause 5 Leadership	• Information Security Policy and Procedures • Information Security Objectives • Information Security Organization Structure, Roles, and Responsibilities (including Segregation of Duties)
			Clause 7 Support, Annex 5.1-5.6	• Security Resource Plan (e.g. tools, human resource, budget, training, special interest group, communication)
Phase A: Architecture Vision	• Approved Statement of Architecture Work	• Obtain management support for security measures	Clause 4 Context of Organization	• Context of Organization (scope of ISMS, constraints,

TOGAF® ADM Phase	Relevant TOGAF® ADM Outputs/ Artifacts (TOGAF®, 2018)	TOGAF® Guidelines & Techniques: Security and ADM (TOGAF®, 2018)	ISO27001:2022 Requirements Mapping	
			References	Security Artifacts
	• Refined statements of business principles, business goals, and business drivers • Architecture Vision • Architecture Definition Document	• Define necessary security-related management sign-off milestones of this architecture development cycle • Identify and document the anticipated physical/business/regulatory environment(s) in which the system(s) will be deployed • Determine and document the criticality of the system: safety-critical/mission-critical/non-critical		and stakeholders)
			Clause 5 Leadership	• Information Security Policy and Procedures
			Clause 6 Plan	• Information Security Plan (including risks, opportunities, strategies, and schedule)
			Clause 7 Support	• Security Resource Plan (e.g. tools, human resource, budget, training, communication)
			Annex 5.3 ICT Readiness for Business Continuity	• Business Continuity Plan • Disaster Recovery Plan
Phase B: Business Architecture	• Architecture Business Baseline • Architecture Business Target	Security Outputs: • List of forensic processes • List of new disaster recovery and business continuity requirements • Validated business and regulatory environment statements • List of validated security policies and regulations • List of target security processes	Clause 8.2 Information Security Risk Assessment, Clause 8.3 Information Security Risk Treatment	• Information security risk assessment • Information security risk controls and mitigating plan • Business Impact Analysis
			Annex 5.7 Threat Intelligence	• Threat intelligence
			Annex 5.9 Inventory of information	• Assets register (including

TOGAF® ADM Phase	Relevant TOGAF® ADM Outputs/ Artifacts (TOGAF®, 2018)	TOGAF® Guidelines & Techniques: Security and ADM (TOGAF®, 2018)	ISO27001:2022 Requirements Mapping	
			References	Security Artifacts
		• List of baseline security processes • List of security actors • List of interconnecting systems • Statement of security tolerance for each class of security actor • Asset list with values and owners • List of trust paths • Availability impact statement(s) • Threat analysis matrix	and other associated assets	asset's user/owner)
			Annex 5.24-Annex 5.29 Information security incident management	• Information security incident management procedures
			Annex 5.10-5.11, Annex 6 (All)	• Human resource-related security controls • Information security incident management procedures
Phase C: Information Systems Architecture	• Architecture Data and Application Baseline • Architecture Data and Application Target	Security Outputs: • Event log-level matrix and requirements • Risk management strategy • Data lifecycle definitions • List of configurable system elements • Baseline list of security-related elements of the system • New or augmented security-related elements of the system • Security use-case models: Normative models Non-normative models	Annex 5.12-5.14	• Information Classification • Data protection and loss prevention (including information transfer rules)
			Annex 5.32	Intellectual Property (IP) Rights
			Annex 5.34	Data privacy policy
			Annex 5.37	Data management life cycle procedures
			Annex 5.33, Annex 8.1-8.12	Data protection and loss prevention
			Annex 5.8	Project management security controls
			Annex 8.25-8.34	Secure coding policy and

TOGAF® ADM Phase	Relevant TOGAF® ADM Outputs/ Artifacts (TOGAF®, 2018)	TOGAF® Guidelines & Techniques: Security and ADM (TOGAF®, 2018)	ISO27001:2022 Requirements Mapping	
			References	**Security Artifacts**
		• List of applicable security standards: Protocols Object libraries Others ... • Validated interconnected system list • Information classification report • List of asset custodians • Function criticality statement • Revised disaster recovery and business continuity plans • Refined threat analysis matrix		application controls
			Annex 5.9 Inventory of information and other associated assets	Assets register (including information/data and applications/software assets)
Phase D: Technology Architecture		• List of security-related elements of the system • List of interconnected systems • List of applicable security standards • List of security actors • Risk management strategy • Validated security policies • Validated regulatory requirements • Validated business policies related to trust requirements	Annex 5.15-5.18	Access control and identity management
			Annex 5.19-5.22	Supplier management
			Annex 5.23	Cloud services security controls
			Annex 5.9 Inventory of information and other associated assets	• Assets register (including hardware/physical assets)
			Annex 7 (All)	• Physical security controls (including security of working areas and data center) • Supporting utilities (e.g. power, cabling, data

TOGAF® ADM Phase	Relevant TOGAF® ADM Outputs/ Artifacts (TOGAF®, 2018)	TOGAF® Guidelines & Techniques: Security and ADM (TOGAF®, 2018)	ISO27001:2022 Requirements Mapping	
			References	**Security Artifacts**
				center supporting equipment)
			Annex 8.1-8.9	• User end point security controls • Access control and identity management • Capacity management • Configuration management • Malware protection
			Annex 8.15-8.19	• OS-level security controls
			Annex 8.2-8.23	Network monitoring and security controls
			Annex 8.24	Cryptography
Phase E: Opportunities and Solution	Opportunities and Solutions Document	• Identify existing security services available for re-use • Engineer mitigation measures addressing identified risks • Evaluate tested and re-usable security software and security system resources • Identify new code/resources/assets that are appropriate for re-use • Determine "what can go wrong?"	No specific security-requirements are mapped to this TOGAF® ADM phase.	
Phase F: Migration Planning	Architecture Roadmap, Implementation and Migration Plan	• Identify existing security services available for re-use	No specific security-requirements are mapped to this TOGAF® ADM phase.	

TOGAF® ADM Phase	Relevant TOGAF® ADM Outputs/ Artifacts (TOGAF®, 2018)	TOGAF® Guidelines & Techniques: Security and ADM (TOGAF®, 2018)	ISO27001:2022 Requirements Mapping	
			References	**Security Artifacts**
		• Engineer mitigation measures addressing identified risks • Evaluate tested and re-usable security software and security system resources • Identify new code/resources/assets that are appropriate for re-use • Determine "what can go wrong?"		
Phase G: Implementation Governance	Architecture Contract, Compliance Assessment	• Establish architecture artifact, design, and code reviews and define acceptance criteria for the successful implementation of the findings • Implement methods and procedures to review evidence produced by the system that reflects operational stability and adherence to security policies • Implement necessary training to ensure correct deployment, configuration, and operations of security-relevant subsystems and components; ensure awareness training of all users and non-privileged operators of the system and/or its components • Determine "what has gone wrong?"	Clause 9.1 Monitoring, measurement, analysis and evaluation	• Security Monitoring
			Clause 9.2 Internal audit, Annex 5.35 Independent review of information security, 5.36 Compliance	• Regular internal audit • Information security independent review
			Clause 9.3 Management Review	• Management review
			Clause 7.3 Awareness Annex 6.3 Information security awareness, education and training	• Information Security training and awareness

TOGAF® ADM Phase	Relevant TOGAF® ADM Outputs/ Artifacts (TOGAF®, 2018)	TOGAF® Guidelines & Techniques: Security and ADM (TOGAF®, 2018)	ISO27001:2022 Requirements Mapping	
			References	Security Artifacts
Phase H: Architecture Change Management	• Request for changes • Architectural or other components changes	Incorporate security-relevant changes to the environment into the requirements for future enhancement (enhancement of existing objective)	Clause 10. Improvement	• Continual improvement

4. Limitation and Opportunity for Future Research

While this paper introduces the SAFE as a promising approach to integrating ISO 27001 standards with the TOGAF® framework, SAFE was developed through a systematic literature review, framework artifact mapping, and analysis based on the writers' professional experiences in information security and EA. Therefore, SAFE is a conceptual framework and requires empirical evidence to support its effectiveness and practical relevance. Moreover, there is a need for research concerning the application of SAFE within specific industry contexts for tailored frameworks. Through empirical validation and iterative refinement, the framework can evolve into a valuable tool for industry practitioners in the EA and information security fields.

5. Conclusion

This paper has introduced the Security Architecture Framework for Enterprises (SAFE) as an approach to integrating ISO 27001 standards with the TOGAF® framework for enterprise architecture. By addressing the challenges of ISO 27001 implementation and providing a structured approach to integration, SAFE offers a valuable solution for organizations seeking to enhance their information security posture in the face of evolving cyber threats.

Through a systematic literature review and framework artifact mapping, we have demonstrated how EA, particularly TOGAF®, can play a strategic role in aligning security initiatives with business goals, optimizing resource utilization, facilitating organizational change management, and managing the complexity of the IT landscape. The proposed integration approach of ISO 27001 requirements into TOGAF® ADM provides a practical framework for organizations to follow, ensuring that security considerations are embedded throughout the architecture development process.

However, it is important to acknowledge the limitations of SAFE as a conceptual framework and the need for empirical validation and tailored application within specific industry contexts. Future research should focus on testing and refining the framework through real-world implementation, as well as exploring its application in different industries and organizational settings. Overall, SAFE has the potential to evolve into a valuable tool for industry practitioners,

offering actionable insights and solutions to integrate security controls within enterprise architectures and enable effective implementation in an increasingly digitalized world.

References:

AbuSaad, B., Saeed, F. A., Alghathbar, K., & Khan, B. (2011). Implementation of ISO 27001 in Saudi Arabia–obstacles, motivations, outcomes, and lessons learned.

Alshitri, K. I., & Abanumy, A. N. (2014). Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia. In *2014 International Conference on Information Science & Applications (ICISA), Information Science and Applications (ICISA), 2014 International Conference on* (pp. 1-4): IEEE.

Andrews, C., Monk, C., & Johnston, R. (2014). Integrated Architecture Framework and Security Risk Management for Complex Systems. *IET Conference Proceedings*, 1.2.1-1.2.1. https://digital-library.theiet.org/content/conferences/10.1049/cp.2014.0965

Anttila, J., Jussila, K., Kajava, J., & Kamaja, I. (2012). Integrating ISO/IEC 27001 and other Managerial Discipline Standards with Processes of Management in Organizations. *2012 Seventh International Conference on Availability, Reliability and Security, Availability, Reliability and Security (ARES), 2012 Seventh International Conference on*, 425-436. https://doi.org/10.1109/ARES.2012.93

Atay, S., & Masera, M. (2011). Challenges for the security analysis of Next Generation Networks. *information security technical report*, *16*(1), 3-11. https://doi.org/https://doi.org/10.1016/j.istr.2010.10.010

Barraza de la Paz, J. V., Rodríguez-Picón, L. A., Morales-Rocha, V., & Torres-Argüelles, S. V. (2023). A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0. *Systems*, *11*(5), 218. https://www.mdpi.com/2079-8954/11/5/218

Beckers, K., Schmidt, H., Kuster, J.-C., & Faßbender, S. (2011). Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing. *2011 Sixth International Conference on Availability, Reliability and Security, Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*, 327-333. https://doi.org/10.1109/ARES.2011.55

Broderick, J. S. (2006). ISMS, security standards and security regulations. *information security technical report*, *11*(1), 26-31.

Dam, H. K., Lê, L.-S., & Ghose, A. (2016). Managing changes in the enterprise architecture modelling context. *Enterprise Information Systems*, *10*(6), 666-696.

Dzazali, S., Sulaiman, A., & Zolait, A. H. (2009). Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. *Government Information Quarterly*, *26*(4), 584-593.

Everett, C. (2011). Is ISO 27001 worth it? *Computer Fraud & Security*, *2011*(1), 5-7. https://doi.org/10.1016/S1361-3723(11)70005-7

Ganji, D., Kalloniatis, C., Mouratidis, H., & Gheytassi, S. M. (2019). Approaches to develop and implement iso/iec 27001 standard-information security management systems: A systematic literature review. *Int. J. Adv. Softw*, *12*(3).

Ganji, D., Mouratidis, H., & Gheytassi, S. M. (2019). Towards a modelling language for managing the requirements of ISO/IEC 27001 standard. 5th International Conference on Advances and Trends in Software Engineering (SOFTENG). Valencia, Spain: IARIA,

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. In *The TQM Journal* (Vol. 23, pp. 367-376): Emerald Group Publishing Limited.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, *16*(4), 377-397.

Haris, L. (2018). Risk Assessment on Information Asset an academic Application Using ISO 27001. *2018 6th International Conference on Cyber and IT Service Management (CITSM)*, 1-4. https://doi.org/https://doi.org/10.1109/CITSM.2018.8674294

Identity Theft Resource Center. (2024). *2023 Data Breach Report*. https://www.idtheftcenter.org/publication/2023-data-breach-report/

ISO. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements. In *ISO/IEC 27001:2022*. International Organization for Standardization.

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information security management standard: how to extract value from data in the IT sector. *Sustainability*, *15*(7), 5828.

Kotusev, S. (2018). TOGAF-based Enterprise Architecture Practice: An Exploratory Case Study. *Communications of the Association for Information Systems*, *43*, 321-359. https://doi.org/10.17705/1CAIS.04320

Loft, P., He, Y., Janicke, H., & Wagner, I. (2019). Dying of a hundred good symptoms: why good security can still fail - a literature review and analysis. *Enterprise Information Systems*, *15*(4), 448-473. https://doi.org/10.1080/17517575.2019.1605000

Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. *2023 International Conference On Cyber Management And Engineering (CyMaEn)*, 117-122. https://doi.org/https://doi.org/10.1109/CyMaEn57228.2023.1005111

Mirtsch, M., Kinne, J., & Blind, K. (2020). Exploring the adoption of the international information security management system standard ISO/IEC 27001: a web mining-based analysis. *IEEE Transactions on Engineering Management*, *68*(1), 87-100.

Neubauer, T., Ekelhart, A., & Fenz, S. (2008). Interactive selection of ISO 27001 controls under multiple objectives. *IFIP – The International Federation for Information Processing*, *278*, 477-492. https://doi.org/https://doi.org/10.1007/978-0-387-09699-5_31

Quartel, D., Steen, M. W., & Lankhorst, M. M. (2012). Application and project portfolio valuation using enterprise architecture and business requirements modelling. *Enterprise Information Systems*, *6*(2), 189-213.

Shariati, M., Bahmani, F., & Shams, F. (2011). Enterprise information security, a review of architectures and frameworks from interoperability perspective. *Procedia Computer Science*, *3*, 537-543. https://doi.org/10.1016/j.procs.2010.12.089

Soliman, W., & Ojalainen, A. (2023). Conflict resolution in an ISO/IEC 27001 standard implementation: a contradiction management perspective.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

The Open Group. (2011). TOGAF® and SABSA® Integration. In: The Open Group and The SABSA Institute.

The Open Group. (2018). TOGAF® Standard Version 9.2. In: Van Haren Group.

Velasco, J., Ullauri, R., Pilicita, L., Jacome, B., Saa, P., & Moscoso-Zea, O. (2018). Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry. *2018 International Conference on Information Systems and Computer Science (INCISCOS)*, 294-300. https://doi.org/https://doi.org/10.1109/INCISCOS.2018.00049