Scientific Research Publishing

Open Journal of Safety Science and Technology, 2024, 14, 96-115
https://www.scirp.org/journal/ojsst
ISSN Online: 2162-6006
ISSN Print: 2162-5999

Security Policy Model in a Hybrid Zachman-TOGAF Framework for a Telework Enterprise Architecture in a Cloud Environment

Pacôme Brou[1], Thomas Kouassi[1,2], Beman Hamidja Kamagate[1], Olivier Asseu[1,2], Yvon Kermarrec[3]

[1]Equipe MAC, Laboratoire LASTIC, Ecole Supérieure Africaine des TIC (ESATIC), Abidjan, Côte d'Ivoire
[2]UMRI STI, Ecole Doctorale Polytechnique, Institut National Polytechnique Houphouët-Boigny, Yamoussoukro, Côte d'Ivoire
[3]Departement Informatique, Institut Mines Telecom Atlantique, Brest, France
Email: broupacom@hotmail.fr

How to cite this paper: Brou, P., Kouassi, T., Kamagate, B.H., Asseu, O. and Kermarrec, Y. (2024) Security Policy Model in a Hybrid Zachman-TOGAF Framework for a Telework Enterprise Architecture in a Cloud Environment. *Open Journal of Safety Science and Technology*, **14**, 96-115.
https://doi.org/10.4236/ojsst.2024.143008

Received: September 1, 2024
Accepted: September 21, 2024
Published: September 24, 2024

Abstract

Context and motivation: In an ever-changing post COVID-19 world, more and more businesses are adopting teleworking models, making it essential to use Cloud technology to facilitate collaboration and data accessibility. However, this transition to teleworking and the Cloud poses major challenges in terms of the security of organization's information systems. Protecting sensitive data and IT systems is becoming an absolute priority to guarantee business continuity and prevent potential cyber threats and attacks. Security policies need to be put in place. Problem: Within a Hybrid Zachman-TOGAF Framework for an Enterprise Architecture exploiting Cloud technology in a teleworking context, several problems arise, including: How can the confidentiality, integrity and availability of the company's critical data be ensured in a teleworking environment using Cloud solutions? Objective and methodology: With this in mind, this article proposes a systemic approach based on a mathematical optimization model to identify, assess and manage information security risks under budgetary constraints to ensure adequate protection of confidential data. The aim is to create a secure, reliable and resilient working environment, where employees can access the necessary resources with confidence, even outside the organization's premises. Results: The approach proposed in this article shows how a mathematical model can be used to optimize security decisions in a cloud environment within a dedicated teleworking enterprise architecture. By integrating these results into a hybrid Zachman-TOGAF Framework, the organization can align its security strategies with its business

objectives, while respecting budgetary constraints and minimizing risk. In addition, Monte Carlo simulations over 10,000 iterations to assess variations in residual risk as a function of fluctuations in threat probabilities and the costs of security measures in the same mathematical model show a trade-off between the cost of implementing the security measure, budget availability and residual risk, which is an aid to decision-making and strategic choices for the system operating in the organization in terms of information system security.

Keywords

Security Policy, Zachman-TOGAF Framework, Residual Risk, Cloud, Teleworking

1. Introduction

For 3000 years, mankind has felt the need to hide and conceal personal or confidential information, long before the computer age. The aim was to protect the content of messages from the inevitable curious onlookers (for example, Caesar's code studied in cryptography in the 1st century BC). This objective is still relevant today, especially as information systems have become essential to the survival of organizations. With threats on the rise, it is essential to ensure their security. Historically, information systems security has been a variant of IT security. This has been a particularly strong need in critical sectors (banking, defense, etc.). IT security is the ability of a system to protect its objects from modification or use by unauthorized parties. With the advent of open networks and the democratization of the Internet, a new context has emerged in which security has taken on a more global dimension: information systems security. In an ever-changing digital world, the security of information systems has become a major concern for organizations, particularly in the context of teleworking and the growing use of Cloud environments. To guarantee the confidentiality, integrity and availability of sensitive data processed remotely, it is essential to put in place a robust and appropriate IT security policy. The use of a hybrid framework combining the complementary approaches of ZACHMAN and TOGAF offers a multidimensional and structured perspective for tackling the complex challenges of IT security. By integrating ZACHMAN's conceptual models with TOGAF's structured phases, it is possible to develop a holistic security policy that is aligned with the organization's strategic needs. According to a study carried out by IBM, the average cost of a data breach for a company is 3.86 million dollars. It is therefore essential to invest in robust security policies to avoid such financial and reputational consequences [1]. Malicious intent has also become an inescapable factor and has taken on considerable proportions through various forms of attack. These attacks range from simple computer malware to cybercrime and threats to the security of critical infrastructures. There are so many attacks on

information systems today that it would be illusory to try to describe them all. This article presents a mathematical optimization model that optimizes the risk incurred by an organization's information system under budgetary constraints in an enterprise architecture under the aegis of a Hybrid Zachman-TOGAF Framework in a teleworking context. The aim is to assess and manage information security risks under budgetary constraints, to ensure adequate protection of confidential data. In the following section, a bibliographical review is developed to better structure the research work in this article.

2. Related Works

Security of an information system comes down to guaranteeing the basic factors of security It is based on three criteria:

- Confidentiality of information.
- System integrity.
- Availability of services.

These three properties are essential for defining an organization's security policy. There are other factors such as proof and control which guarantee audibility and non-repudiation. Confidentiality is the property of information that is neither available nor disclosed to unauthorized persons, entities or processes. It means determining the authorized users and the limits of their prerogatives [2]. Formulating requirements for the confidentiality of information is tantamount to setting out criteria on which to base the legitimacy of access to this information [3], among others:

- User-related criteria: Identity, group membership, authorization, etc.
- Function-related criteria: Rights, authorizations, need-to-know, need-to-use, etc.
- Role-related criteria: Responsibilities, delegations, requirements, etc.

The security of information systems has always been a key factor in the survival of any organization. Within the literature, several writings have been devoted to this issue, in this regard the work of [4] present a paper on the guidelines for the development of information security and experiences on the process of developing information security policies in higher education institutions facing the challenges of cybersecurity due to information cultures and open computing resources on campuses; According to [5], information security policy is a solution for guaranteeing data security using an appropriate model for assessing compliance with information security policy, and this understanding will undoubtedly improve predictions of the impact of compliance with information security policies, In the same vein, Clark [6] assert that the adoption of online platforms for distance learning is a means of exposing university information systems to cybercrime activities carried out by internal and external agents of malicious users whose aim is data acquisition, for countermeasure they propose a security model for data security and protection through empirical studies relating to security policies on the use of online platforms in order to prevent them

from being exposed to malicious users. The different security policies studied in the literature have also led to the definition of different classes of security models among others: survey-based security policy for small organizations [7], The three-dimensional model of the security management and control system built from viewpoints such as process control, resource protection and the achievement of security objectives based on the characteristics of the information system in IT governance [8], The multi-level security policy essentially consists of dividing information into different security levels and adopting different protection measures depending on the security level [9], The policy model based on internal controls and IT risk governance to ensure that corporate guidelines, such as security policies, standards, procedures, guidelines, business rules and practices at all levels of the organization, are correctly selected and adapted to the organization [10], an automata-based security policy for network security functions [11], in 2021, [12] improve the security policy proposed by [11], by adding an automatic data model mapper, in fact the proposed mapper focuses on the mapping between high-level data model elements and low-level data model elements in order to automate the translation without the need for a security administrator to create a mapping table. These different policies are built based on a security model, the aim of which is to clearly define in mathematical language what the security policy describes, and are generally based on the concepts of subjects, objects and permissions. These models generally define three types of access: read (consultation/reading), write (modification/writing) and execute (execution), and these rights can apply either to the owner of the file, or to a group of users, or to other users; Indeed:

- If S_1 is a subject running on behalf of the user U_1 file owner f_1, it can give subject S_2 (running on behalf of U_2) the right to read f_1:

$$(S_1, f_1, \text{owner}) \rightarrow (S_2, f_1, \text{read}) \tag{1}$$

- S_2 can create a file f_2 (in which he can write) on which he can give read access to S_3 (running on behalf of U_3):

$$(S_2, f_2, \text{create}) \rightarrow (S_2, f_2, \text{read}) \wedge (S_3, f_2, \text{read}) \tag{2}$$

- S_3 can then copy f_1 into f_2 to transmit information to f_1 à S_3 without the Owner's knowledge S_1:

$$(S_2, f_1, \text{read}) \wedge (S_2, f_2, \text{write}) \wedge (S_3, f_2, \text{read}) \rightarrow (S_3, k(f_1), \text{read}) \tag{3}$$

where $k(f_1)$: copy of f_1.

A discretionary authorization policy is therefore only applicable insofar as it is possible to fully trust users and the subjects who perform on their behalf. Such a policy is therefore vulnerable to abuse of power caused by clumsiness or malice.

In addition to the models mentioned above, there are other specific models developed to represent a particular authorization policy:

- Lattice-based models, which assign each user and each object a specific security level; this type of model has been associated with the multi-level policies

of [13] and [14].

- Other (generally less formalized) models, such as [15] model developed for commercial organizations, [16] Chinese wall model designed to represent conflicts of interest in financial institutions, or [17] role-based models, adapted to several types of organization, use roles as an intermediary entity between subjects and permissions.

Information system's position at the heart of the organization and its information processing function make it an important element to protect for the organization's survival.

With Industry 4.0, massive, heterogeneous data can pose a danger to the IS. Big Data is collected, processed and stored using heterogeneous instruments; These specificities are not taken into account when assessing cybersecurity and resilience, if conventional security assessment techniques based on static, ontological, neural network, risk-oriented or other types of analysis are applied to resolve this shortcoming, Kalinin and Poltavtseva in 2024 at the "International Russian Smart Industry" conference proposed a new Big Data security assessment technique that uses a data processing graph and bidirectional data access analysis, the results of which show that it performs compliance of actual access capabilities with the given access control policy [18]. One of the most difficult security issues to resolve in the cloud is to define and manage different levels based on the concepts of isolation, service provision and cloud scalability. These security levels must be protected against disclosure to unauthorized users. Cloud and its security and privacy issues, as well as countermeasures, are one of the most hotly debated topics in today's IT industry, with suggested policy models advocating per-level security management in the cloud, access to which is modeled by a set of permissions as follows:

Let be a set of subjects *S*, a set of objects *o*, an access matrix *M* and a Functions giving the level *f*. A set of access permissions is also available $A=\{e,r,a,w\}$. They are classified according to their ability to observe (read) and alter (write) information:

- *e*: Neither observation nor alteration (Run);
- *r*: Unaltered observation (Read);
- *a*: Alteration without observation (Append).
- *w*: Observation et alteration (Write).

Then:

- $r\in M[s,o]\Rightarrow f(s)\geq f(o)$ (4)
- $a\in M[s,o]\Rightarrow f(s)\leq f(o)$ (5)
- $w\in M[s,o]\Rightarrow f(s)=f(o)$ (6)

These laws mean:

- (4) For a subject s to have read access to an object *o*, its clearance level f(s) must be greater than or equal to the object's classification level $f(o)$.
- (5) For a subject to have write access to an *o* object, its clearance level must

be less than or equal to the object's classification level.

- (6) For a subject to have read/write access to an *o* object, his or her clearance level must be equal to the object's classification level.

The safety objectives of this policy are:

- Law 1: Prohibit any propagation of information from an object at a certain integrity level to an object at a higher integrity level.
- Law 2: Prohibit any subject at a certain integrity level from modifying an object with a higher integrity level.

These two-level laws can be modeled as follows:

- $r \in M[s,o] \Rightarrow f(s) \leq f(o)$ (7)
- $a \in M[s,o] \Rightarrow f(s) \geq f(o)$ (8)
- $w \in M[s,o] \Rightarrow f(s) = f(o)$ (9)

These rules prevent the transfer of information from a low integrity level to a high integrity level, which would compromise the integrity of the high level. In the same vein, Fatemi Moghaddam has proposed a reliable access management framework based on multi-level policies and sequences, the results of which enable access response times to be reduced without affecting the security of environments [18]. Livshitz *et al.* describe a method for assessing the level of information security in a credit organization, the results of which can be used to assess compliance with the credit organization's IT security requirements [19].

In addition to this research work, we have a complete security policy framework based on a network topology as part of the Government services in Bangladesh whose aim is to provide a secure network to remote areas [20]. The various security policies mentioned above all have the same security objectives, *i.e.* the desired confidentiality, integrity and availability properties of the system, so any action, whether deliberate or accidental, that could undermine one of these properties must be intercepted and processed by a global security policy applicable to all entities. The state of the art on information systems security has enabled us to address the fundamentals and concepts of IS security, but the whole issue of securing an organization whose architecture is based on a Hybrid Framework in a telecommuting context has not been tackled. This article therefore proposes a mathematical model enabling us to optimize the level of risk incurred in the system under the constraint of respecting the budget dedicated to securing it. The following section details the methodology and properties used to define this model.

3. Materials and Methods

3.1. Materials

Hardware 1: creating a security policy template for the Zachman-TOGAF Hybrid Framework. To implement a security policy in a Hybrid Zachman-TOGAF Framework, you need:

- The ZACHMAN perspective matrix
- The components of the TOGAF approach

This involves a series of strategic steps to effectively align security objectives with the organization's architectural and operational requirements. Both frameworks are necessary to create a matrix that ensures security policies are addressed in a comprehensive and integrated way at every level of the architecture. In a cloud environment, IT security must be adapted to meet the specific challenges of the cloud, such as access management, data protection and compliance.

Hardware 2: Modeling a budget-constrained optimization model

To test the mathematical model, we'll need:

- Data: The dataset comes from a Kaggle cybersecurity attack database. It covers the period from January 1, 2020 to October 11, 2023. This dataset contains 40,000 data records with 25 various metrics https://www.kaggle.com/datasets/teamincribo/cyber-security-attacks/data.
- Software: python 3, power BI and Monte Carlo Method.

Python (with libraries such as NumPy, SciPy) is used to extract the columns from the dataset required for experimentation, to create different possible scenarios and generate costs.

Power BI: Drawing up a dashboard after data cleansing in Power Query to identify attack types and frequencies. Three types of attack are identified in the database: DDoS, malware and intrusion.

Monte Carlos: For statistical analysis of residual risks.

3.2. Security Policy Model in a Hybrid Zachman-TOGAF Framework

3.2.1. Definition of the IT Security Policy Matrix in a Hybrid Zachman-TOGAF Framework in a Cloud Environment

Design of the matrix involves combining Zachman's multidimensional structure with TOGAF's iterative architecture development process. The structuring of this matrix is organized according to Zachman's six fundamental questions (what, how, where, who, when why) and will integrate the relevant phases of TOGAF's ADM cycle for each question. Each cell of the matrix will describe the relevant security policy elements.

- The columns are the Zachman Framework's queries for planning security objectives:
  - What: What data or resources require protection?
  - How: By what technical means or processes are the protections applied?
  - Where: Where are the protections physically and logically implemented?
  - Who: Who is responsible for implementing and managing security?
  - When: When are security measures activated, monitored and reviewed?
  - Why: What compliance and operational objectives do security seek to achieve?
- The TOGAF ADM phases for security development:
  - Phase A (Architecture Vision): Include security objectives in the initial architecture vision to guide all subsequent phases.

- Phases B, C and D (Business Architecture, Information Systems, Technology): Develop specific architectures that incorporate security controls to protect assets at all levels.
- Phase E (Opportunities and Solutions): Identify and evaluate security solution options that meet the requirements identified.
- Phase F (Implementation Planning): Plan the implementation of the security solutions, ensuring that they are integrated into the overall deployment schedule.
- Phase G (Implementation Governance): Monitor security implementation to ensure compliance with defined security policies.
- Phase H (Architecture Change Management): Reviewing and adjusting security measures in response to new threats, technologies and changes in business requirements.

For its definition, this matrix (see Table 1) could be structured as follows to consider the essential aspects of security in a cloud environment:

Table 1. Cloud security policy matrix in a Zachman-TOGAF framework.

		ZACHMAN'S QUESTIONS					
		What?	**How?**	**Where?**	**Who?**	**When?**	**Why?**
ADM ToGAF PHASES	Phase A	Identifying critical data for teleworking	Defining basic safety approaches	-	-	Initiating the safety vision	Align safety with business and compliance objectives.
	Phase B	Details of business assets concerned.	Data classification process.	-	Corporate governance roles.	Periodic revisions.	Ensure the integrity and confidentiality of corporate data.
	Phase C & D	Sensitive application s and data.	Encryption, IAM, network security.	Cloud and on-permise.	IT and security.	Data and application lifecycles.	Protection against data loss and unauthorized access.
	Phase E	-	Selecting security solutions.	Specific deployment zones.	Project teams.	Deployment planning.	Maximizing the efficiency of safety resources.
	Phase F	-	Implementation of security controls.	Critical sites.	Operational staff.	Implementation schedule.	Respecting deadlines and safety budgets.
	Phase G & F	Audit of existing security measures.	Continuous improvement of measurements.	Extension to new regions.	Internal and external audits.	Compliance cycles.	Adapting to new threats and regulations

3.2.2. Mathematical Approach to the Security Policy Model in a Hybrid Zachman-TOGAF Framework in a Cloud Environment in the Context of Teleworking

The move towards teleworking has introduced new challenges for IT security. A mathematical model under a hybrid Zachman-TOGAF Framework is used to formulate and solve complex security problems, integrating Zachman perspectives with TOGAF lifecycle phases.

The model aims to provide a rigorous approach to risk management, data protection and business continuity in a distributed work environment.

The mathematical model of IT security for teleworking can be described by the following elements:

1) Variable and parameter

Let be the following sets:

I: All risks and threats $(i \in I; i = 1, \cdots, n)$

J: The entire safety measure with $(j \in J; J = 1, \cdots, m)$

K: Essential services with $(k \in K; k = 1, \cdots, p)$

x_{ji} : Binary variable associating a corrective measure *j* to the threat *i*

- **Risks and threats specific to the cloud:** Either

- R_i : Level of risk cost associated with the threat *i*, with

$$R = \sum_{i=1}^{n} R_i \tag{10}$$

- P_i : Probability of threat occurrence *i*
- L_i : Expected losses if the threat materializes *i*

- **Cloud security measures**

- $x_{ji} = \begin{cases} 1 \text{ if corrective action } j \text{ is associated with a threat } i \\ 0 \text{ otherwise} \end{cases}$
- C_j : Budget cost of implementing safety measure *j* to counter threat *i*
- S_{ji} : Effectiveness of safety measure *j* in reducing risk *i*

- $S_{ji} = \begin{cases} 1 \text{ if safety measure } j \text{ completely eliminates threat } i \\ 0 \text{ otherwise} \\ \lambda \in]0,1[\text{ is the probability of measure } j \text{ reducing threat } i \end{cases}$ (11)

- **Compliance and regulation**

- $C_{\min}$: Minimum regulatory compliance threshold to be achieved by implementing safety measures
- G_j : Contribution of safety measures *j* to Regulatory Compliance

- **Availability and Performance**

- A_k : Service availability *k* after implementation of security measures
- $A_{\min}$: Minimum availability threshold for critical services.

- **Budget**

- *B*: Total budget available for implementing safety measures

2) Objective function

Objective of the mathematical model is to minimize overall risk while optimizing safety costs and guaranteeing compliance.

- **Fonction Fitness:**

$$\min R = \min \sum_{i=1}^{n} R_i = \sum_{i=1}^{n} P_i * L_i - \sum_{j=1}^{m} \sum_{i=1}^{n} S_{ji} * \left(C_j * x_{ji} \right) \tag{12}$$

This function minimizes potential losses due to risk, while maximizing the cost effectiveness of the security measures implemented.

3) Constraints

- **Budget**: Expenditure on safety measures must not exceed the available budget.

$$\text{s.c} \sum_{j=1}^{m} C_j = C_{total} \le B \tag{13}$$

- **Compliance**: Level of compliance must be at least equal to the minimum threshold required

$$\sum_{j=1}^{m} G_j \ge C_{\min} \tag{14}$$

- **Availability** Security measures must ensure that the availability of critical services is not compromised

$$A_k = A_{\min}, \ \forall k \in K \tag{15}$$

where A_k is the service availability k and $A_{\min}$ is the minimum availability threshold.

1) Translates the objective function to be minimized: The first and second terms represent respectively the total cost-optimizing risk, and the effectiveness of the safety measures deployed to reduce the risk. Constraint 2) imposes that all corrective safety measures must not exceed the Total Budget B allocated to corrective measures., constraint 3) ensures that the solutions chosen must meet a minimum compliance threshold $C_{\min}$, 4) ensures minimum availability of essential services despite the security measures implemented.

4) Mathematical optimization program

Mathematical Program for Combinatorial Optimization of Security Policy in a Hybrid Zachman-TOGAF Framework in a cloud environment in an enterprise architecture dedicated to telecommuting, whose objective is to

$$\begin{aligned} &\min R = \sum_{i=1}^{n} P_i * L_i - \sum_{i=1}^{n}\sum_{j=1}^{m} S_{ji} * \left(C_j * x_{ji}\right) \\ &\text{s.c} \sum_{j=1}^{m} C_j \le B \\ &\sum_{j=1}^{m} G_j \ge C_{\min} \\ &A_k = A_{\min}, \ \forall k \in K, k = 1, \cdots, p \end{aligned} \tag{16}$$

The aim is to minimize the total cost of total risk, while respecting budgetary constraints and maximizing the effectiveness of safety measures and the availability of minimum service for the continuity of the organization's services.

From the Fitness function of this mathematical program set out in (12), residual risk can be calculated R_{r_i} of each threat after application of corrective safety measures

5) Residual risk R_{r_i} calculation after application of corrective measures in the Information System (IS)

Definition:

- Residual risk (R_{r_i}) is the risk existing after the application of safety measures and the budgetary cost associated with the threat i

- Efficiency S_{ij} which is a safety measure j to reduce risk i e is a probability providing three pieces of information about the existence of the threat i in organization. indeed:

Examining (11), one has:

- If $S_{ji}=1$, then $R=0 \Rightarrow R_{r_i}=0$ (17)

This means that the threat is eliminated from the information system

Therefore $C_j = P_i * L_i, \quad j \in J$

- If $S_{ij}=0$, alors $R=R_{r_i}=P_i * L_i$ (18)

This means that the threat i is almost permanent in the information system, so a new policy must be defined to counter the threat.

- If $S_{ij}=\lambda$ où $\lambda \in]0,1[$, Then:

$$R_{r_i} = P_i * L_i - \left(1 - S_{ji}\right) * C_j, \quad \text{avec } i \in I \text{ et } j \in J$$

$$R_{r_i} = P_i * L_i - \left(1 - S_{ji}\right) * P_i * L_i, \quad \text{avec } i \in I \text{ et } j \in J$$

$$R_{r_i} = P_i * L_i * \left(1 - S_{ji}\right), \quad \text{avec } i \in I \text{ et } j \in J \tag{19}$$

This means that there is a residual risk associated with the threat i defined in (19), so decision-makers need to implement security measures to keep the information system running smoothly.

4. Experimentation, Results and Discussions

4.1. Experimentation: Methodology and Test Battery

The test methodology is presented in the following algorithm:

Start

Step 1: Defining simulation scenarios

In this step, threat scenarios are identified (DDoS attack, data breach, unauthorized access, malware) with assumptions such as: network load, number of remote users, or initial security configurations.

Step 2: Setting up the mathematical model

This involves establishing the probability of occurrence of threats P_i the costs of implementing security measures C_j and the levels of risk R_i associated with the threat. These various parameters will be constrained by budgetary limits B, minimum compliance requirements $C_{\min}$ and availability levels $A_{\min}$ which is the minimum availability threshold.

Step 3: Run the Simulation under the listed assumptions

Run the model simulation with the different scenarios defined. Then proceed as follows, analyze results by collecting data on the impact of different safety measures, cost optimization, and the overall effectiveness of strategies.

Step 4: Evaluation, adjustment and validation

Evaluate the results obtained by analyzing the performance of safety strategies in relation to the objectives of risk minimization, compliance and cost; then compare the simulation results with the predefined criteria or, if necessary, iter-

ate on the scenarios with new parameters until optimal results are obtained.

End

4.2. Results and Discussions

4.2.1. Results

The data generated using Python code are shown in Table 2.

Table 2. Optimization model simulation data.

Attacks on information systems			Safety measures and efficiency			Budget availability B for securing the Information System
Threats (i)	Probability of threat occurrence (i), P_i	Loss L_i generated by threats	Measurement of Security j	Budget line C_j dedicated to the implementation of safety measure j:	Probability of control of threat (i), by measurement j: (Efficiency: S_{ji})	
i_1 = DDoS attacks	$P_1 = 0.1$	$L_1 = 300{,}000$	J_1 = Firewall Application	$C_1 = 60{,}000$	$S_{11} = 0.7$	
i_2 = Intrusion or unauthorized access	$P_2 = 0.25$	$L_2 = 400{,}000$	J_2 = Data encryption (CD)	$C_2 = 80{,}000$	$S_{22} = 0.8$	$B = 200{,}000$
i_3 = Malware	$P_3 = 0.15$	$L_3 = 600{,}000$	J_3 = Advanced antivirus or software update	$C_3 = 120{,}000$	$S_{33} = 0.85$	

- The threats i identified are: i ={1; 2; 3} = {DDoS attacks; Intrusion or unauthorized access; Malware}.
- Safety measures j to counter threats i are: j = {1; 2; 3} = {Application firewall; Data encryption; Advanced antivirus and software update}.
- Residual risk calculation $R_{r_i} = P_i * L_i * \left(1 - S_{ji}\right)$ in the information system.

It can be seen from Table 3 that the total cost of counter-security measures is higher than Budget Availability B for securing the Information System.

Table 3. Calculation of residual threat risk and counter measure implementation costs.

Threats				**Safety measures and efficiency**			Implementing countermeasures
Type of attack (i)	Probability P_i	Threat impact L_i	Information system risk	Safety measures j	Cost C_j	Efficiency: S_{ji}	Residual Risk R_{r_i}
DdoS attacks	$P_1 = 0.1$	**300,000**	**30,000**	Application firewall	$C_1 =$ **60,000**	$S_{11} = 0.7$	**9000**
Intrusion or unauthorized access	$P_2 = 0.25$	**400,000**	**100,000**	Data encryption	$C_2 =$ **80,000**	$S_{22} = 0.8$	**20,000**
Malware	$P_3 = 0.15$	**600,000**	**90,000**	Advanced antivirus or software update	$C_3 =$ **120,000**	$S_{11} = 0.85$	**13,500**
Total	Cost of information system risk			Cost of counter-measures	Budget availability B for information system security		Information system residual risk
	$\sum_{i=1}^{n} R_i = P_i * L_i = 220000$			$\sum C_j = 260000$	$B = 200000$		$\sum R_{r_i} = 42500$

$$\sum_{j=1}^{m} C_j = 260000 > B = 200000$$

This goes against constraint (2) of Optimization model:

$\sum_{j=1}^{m} C_j \leq B$. Safety measures must therefore be optimized to meet budgetary constraints.

- Optimization of security measures to meet Budget B availability for securing the Information System

- **Scenario 1**: Removal of security measure: Application Firewall

Analysis of Table 4 results:

Table 4. Results of scenario 1 with the "Application Firewall" security measure removed.

Threats				**Safety measures and efficiency**			Implementing countermeasures
Type of attack (i)	Probability P_i	Threat impact L_i	Information system risk	Safety measures j	Cost C_j	Efficiency: S_{ji}	Residual Risk R_{r_i}
DDoS attacks	$P_1 = 0.1$	**300,000**	**30,000**	-	-	-	**30,000**
Intrusion or unauthorized access	$P_2 = 0.25$	**400,000**	**100,000**	Data encryption	$C_2 =$ **80,000**	$S_{22} = 0.8$	**20,000**
Malware	$P_3 = 0.15$	**600,000**	**90,000**	Advanced antivirus or software update	$C_3 =$ **120,000**	$S_{11} = 0.85$	**13,500**
Total	Cost of information system risk			Cost of counter-measures	Budget availability B for information system security		Information system residual risk
	$\sum_{i=1}^{n} R_i = P_i * L_i = 220000$			$\sum C_j = 200000$	$B = 200000$		$\sum R_{r_i} = 63500$

This scenario of removing the "Application Firewall" security measure, while respecting the limits of the budgetary cost dedicated to security, has increased the risk associated with DDoS attacks to 30,000, directly exposing cloud applications to common threats such as: SQL Injection, Cross-Site Scripting (XSS) linked to user data theft, and application-layer DDoS attacks. In addition, this reduces the ability of security teams to react quickly to potential threats and data breaches, resulting in non-compliance with security standards.

Recommendation: If the budget were slightly increased, the company could restore the full application firewall, further reducing the residual risk.

- **Scenario 2**: Withdrawal of security measure: Data encryption

Analysis of the results in Table 5: Reducing the scope of data encryption increased the residual risk of data leakage fivefold but kept the organization within budget. Of course, there is a trade-off, but removing data encryption in a cloud-based telecommuting organization jeopardizes the security of critical information and exposes the organization to legal and financial risks.

Table 5. Results of scenario 2 with the "Data encryption" security measure removed.

Threats				Safety measures and efficiency			Implementing countermeasures
Type of attack (i)	Probability P_i	Threat impact L_i	Information system risk	Safety measures j	Cost C_j	Efficiency: S_{ji}	Residual Risk R_{r_i}
DdoS attacks	$P_1 = 0.1$	**300,000**	**30,000**	Application firewall	C_1 = **60,000**	$S_{11} = 0.7$	**9000**
Intrusion or unauthorized access	$P_2 = 0.25$	**400,000**	**100,000**	-	-	-	**100,000**
Malware	$P_3 = 0.15$	**600,000**	**90,000**	Advanced antivirus or software update	C_3 = **120,000**	S_{11} =0.85	**13,500**
Total	Cost of information system risk			Cost of counter-measures	Budget availability B for information system security		Information system residual risk
	$\sum_{i=1}^{n} R_i = P_i * L_i = 220000$			$\sum C_j = 180000$	$B = 200000$		$\sum R_{r_i} = 122500$

Recommendation: If the budget were slightly increased, the company could reinstate full encryption, further reducing the residual risk

- **Scenario 3**: Removal of security measure: Advanced antivirus or software update

Analysis of the results in Table 6: The removal of advanced antivirus has greatly increased the residual risk of intrusion or unauthorized access. The total residual risk is the highest, which may be critical to the organization in the long term despite the low initial costs (=140,000). For a telecommuting organization using cloud technology, this can have serious consequences in terms of information systems security, including Increased Vulnerability to Malware and Ransomware, Loss of Detection of Advanced Threats, Reduced Protection of Remote Access Points, and Exposure to Internal and External Threats.

Table 6. Result of scenario 3 with the "Data Encryption" security measure removed.

Threats				Safety measures and efficiency			Implementing countermeasures
Type of attack (i)	Probability P_i	Threat impact L_i	Information system risk	Safety measures j	Cost C_j	Efficiency: S_{ji}	Residual Risk R_{r_i}
DdoS attacks	$P_1 = 0.1$	**300,000**	**30,000**	Application firewall	C_1 = **60,000**	$S_{11} = 0.7$	**9000**
Intrusion or unauthorized access	$P_2 = 0.25$	**400,000**	**100,000**	Data encryption	C_2 = **80,000**	$S_{22} = 0.8$	**20,000**
Malware	$P_3 = 0.15$	**600,000**	**90,000**	-	-	-	**90,000**
Total	Cost of information system risk			Cost of counter-measures	Budget availability B for information system security		Information system residual risk
	$\sum_{i=1}^{n} R_i = P_i * L_i = 220000$			$\sum C_j = 140000$	$B = 200000$		$\sum R_{r_i} = 119000$

Recommendation: If the budget were slightly increased, the company could restore full encryption, further reducing the residual risk.

- **Evaluation of residual risk variations as a function of fluctuations in threat probabilities and costs of security measures in the mathematical model**

Residual risk fluctuations are assessed using the Monte Carlo method, which involves generating many random values for threat probabilities and security costs, and then calculating the corresponding residual risks. A test is run for each scenario

Python code is:

```
import numpy as np
import matplotlib.pyplot as plt
# Number of iterations for each scenario
iterations = 10000
# Threat probability distribution (normal distribution)
prob_threat_scenario1 = np.random.normal(0.05, 0.01, iterations)
prob_threat_scenario2 = np.random.normal(0.15, 0.03, iterations)
prob_threat_scenario3 = np.random.normal(0.3, 0.05, iterations)
# Cost distribution of security measures (normal distribution)
cost_security_scenario1 = np.random.normal(150000, 20000, iterations)
cost_security_scenario2 = np.random.normal(100000, 25000, iterations)
cost_security_scenario3 = np.random.normal(50000, 30000, iterations)
# Residual risk calculation for each scenario
risk_residual_scenario1 = prob_threat_scenario1 * cost_security_scenario1
risk_residual_scenario2 = prob_threat_scenario2 * cost_security_scenario2
risk_residual_scenario3 = prob_threat_scenario3 * cost_security_scenario3
# Creation of histograms for each scenario
plt.figure(figsize = (14, 8))
plt.subplot(1, 3, 1)
plt.hist(risk_residual_scenario1, bins = 50, color = 'blue', alpha = 0.7)
plt.title('Scenario 1: Low probability, High cost')
plt.xlabel('Residual Risk (€)')
plt.ylabel('Frequency')
plt.subplot(1, 3, 2)
plt.hist(risk_residual_scenario2, bins = 50, color = 'green', alpha = 0.7)
plt.title('Scenario 2: Average probability, Average cost')
plt.xlabel('Residual Risk (€)')
plt.ylabel('Frequency')
plt.subplot(1, 3, 3)
plt.hist(risk_residual_scenario3, bins = 50, color = 'red', alpha = 0.7)
plt.title('Scenario 3: High probability, Low cost')
plt.xlabel('Residual Risk (€)')
plt.ylabel('Frequency')
plt.tight_layout()
```

plt.show()

Simulation to assess residual risk variations in a mathematical model defined in (16) is used with the following parameters: **Threat probabilities**: Normal distribution centered at 0.2 [0.1 - 0.25] with a standard deviation of 0.05. **Costs of security measures**: Normal distribution centered at 100,000 [60,000 - 120,000] with a standard deviation of 20,000.

The results show the distribution of residual risk calculated as the product of threat probabilities and security costs for each simulation iteration as shown in Figure 1. The histogram illustrates the frequency of different levels of residual risk, enabling a visual analysis of the potential impact of fluctuations in security parameters and threats. This visualization helps to understand the distribution and variance of residual risk, which is crucial for the evaluation of security strategies and decision-making in a secure cloud environment.

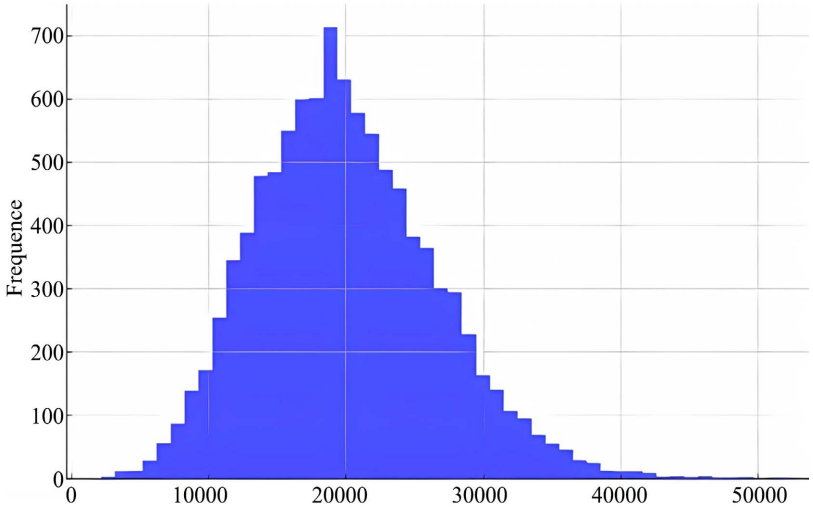

Figure 1. Residual risk distribution using the Monte Carlo method.

Table 7 contains data from Monte Carlo simulation for residual risk, including 20 separate simulations. The generation code is:

Table 7. Residual risk calculated based on threat probabilities and safety costs.

Simulation Number	Threat Probability	Security Cost	Residual Risk
1	0.224	129,313	21,422
2	0.193	95,484	20,082
3	0.232	101,351	15,124
4	0.276	71,505	14,070
5	0.188	89,112	14,656
6	0.188	102,218	20,849
7	0.279	76,980	17,442
8	0.238	107,514	30,361

Continued

9	0.177	87,987	23,289
10	0.227	94,166	9742
11	0.177	87,966	23,183
12	0.177	137,046	23,634
13	0.212	99,730	16,496
14	0.104	78,846	30,274
15	0.114	116,541	11,975
16	0.172	75,583	28,709
17	0.149	104,177	16,079
18	0.216	60,807	17,350
19	0.155	73,436	22,054
20	0.129	103,937	14,989

```
import numpy as np
import pandas as pd
# Setting a seed for reproducibility
np.random.seed(42)
# Generating data for a Monte Carlo simulation for 20 lines
data = {
    "Simulation Number": range(1, 21),
    "Threat Probability": np.random.normal(0.2, 0.05, 20),
    "Security Cost (€)": np.random.normal(100000, 20000, 20),
    "Residual Risk (€)": np.random.normal(0.2, 0.05, 20) *
np.random.normal(100000, 20000, 20)
}
# Creating a DataFrame
df = pd.DataFrame(data)
# Displaying the DataFrame
Df
```

Analysis of the results in Table 7 shows that threat probability values vary mainly around the initial mean of 0.2, with a normal distribution as expected. The cost of security also varies according to a normal distribution around 100,000.

Residual risk values show a wide range, reflecting the interaction between threat probability and security cost.

These data clearly illustrate how variations in inputs (threat probabilities and security costs) affect residual risk, which is crucial for planning and optimizing risk management strategies in a financial environment (under budgetary constraints).

4.2.2. Discussions

The implementation of a hybrid Zachman-TOGAF Framework in an enterprise

architecture where the organization of work is based on telecommuting plays a crucial role in information system risk management; indeed, this type of Framework combines the structural principles of Zachman with the development and management process of TOGAF, enabling a comprehensive and systematic approach to enterprise architecture. In terms of risk management, it helps to provide a classification model that helps to define and visualize all the organization's IT assets (applications, data, infrastructure), as well as their interactions. This helps to identify areas at risk, and to understand how changes in one area may impact on others. By integrating business objectives into IT architecture design (a central approach in both Frameworks), companies can better assess and manage the risks associated with non-compliance with business and regulatory requirements. This is essential for telecommuting organizations, where normal security controls may be less rigorous. The Framework guides the development of security policies and procedures tailored to the cloud and teleworking, specifically addressing aspects of data security, access control and identity management. Structuring continuity plans according to Zachman's categories ensures that all aspects of the business are considered, reducing residual risks in the event of an outage or incident. The risk assessment process is integrated into every phase of the TOGAF lifecycle, from architecture design to implementation. Zachman helps visualize the impact of each risk at different levels (operational, tactical, strategic), enabling more targeted and effective mitigation. This enables organizations to adapt to new threats and technologies without compromising security or performance. As for the mathematical optimization model, it can systematically quantify the risks associated with the various aspects of telecommuting and the cloud environment under budgetary constraints. Using quantitative data, the model identifies and evaluates risks and residual risks by estimating the probability and potential impact of various threats and assesses how risks in certain areas (such as data security) may affect other aspects of the organization. Its integration into the Zachman-TOGAF Framework helps place security aspects within the structured Zachman framework, aligning security objectives with different perspectives (operational, system, technological, etc.) and when using TOGAF's Architecture Development Method (ADM), the mathematical model provides quantitative data that can be used to inform decisions at every stage of the architecture development process. With Monte Carlo, the generation of failure scenarios and other potential crises helps managers to better understand how these events could affect operations, and plan business continuity and disaster recovery accordingly. The aim is to test the effectiveness of security strategies against hypothetical scenarios in order to prepare and reinforce defenses, which will certainly enable security policies to be adjusted. With data based on a wide range of possible outcomes, Monte Carlo simulations reduce uncertainty while increasing confidence in risk management decisions. This is particularly valuable in dynamic and rapidly evolving environments such as the cloud.

5. Conclusion

IT security is of paramount importance for any company operating in a digital environment, and even more so in today's teleworking environment, where sensitive data is frequently exchanged remotely. The implementation of a mathematical risk management model and an appropriate security policy, integrated within the Zachman-TOGAF Hybrid Framework, is a guarantee of protection for the organization's strategic information and digital assets. At the heart of this approach is the identification of critical assets, the definition of protection strategies, and the implementation of control and monitoring mechanisms. The merging of the Zachman and TOGAF models, and the various simulation scenarios carried out, offer a global perspective on enterprise architecture, enabling security strategy to be aligned with organizational objectives, while guaranteeing effective management of the risks associated with the use of Cloud technology.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Cybersector (2024) Data Breach, What Cost, Impact and Mitigation Measures for Your Business in 2024. https://cyberspector.com/violation-des-donnees-quel-cout-impact-et-mesures-dattenuation-pour-votre-entreprise-en-2024/

[2] Donald, L.P. (2000) Information Systems Security, Global Corporate Protection. Campus Press.

[3] Barbara, G and Edward, R. (1995) An Introduction to Computer Security: The NIST Handbook. https://doi.org/10.6028/NIST.SP.800-1

[4] Bell, D.E. and LaPadula, L.J. (1976) Secure Computer Systems: Unified Exposition and Multics Interpretation. Technical Report, MTR 2997 Rev. 1, MITRE Corp.

[5] Biba, K.J. (1977) Integrity Consideration for Secure Computer Systems. The MITRE Corporation, Technical Report ESD-TR-76-372 & MTR-3153.

[6] Clark, D.D. and Wilson, D.R. (1987) A Comparison of Commercial and Military Computer Security Policies. 1987 *IEEE Symposium on Security and Privacy*, Oakland, 27-29 April 1987, 184. https://doi.org/10.1109/sp.1987.10001

[7] Brewer, D.F.C. and Nash, M.J. (1989) The Chinese Wall Security Policy. *Proceedings* 1989 *IEEE Symposium on Security and Privacy*, Oakland, 1-3 May 1989, 206-214. https://doi.org/10.1109/secpri.1989.36295

[8] Ismail, W.B.W., Widyarto, S., Adiyarta, K., Syafrullah, M. and Tajuddin, L.M. (2022) An Information Security Policy Development Process in Higher Education Institution: A Case Study Approach. 2022 9*th International Conference on Electrical Engineering*, *Computer Science and Informatics* (*EECSI*), Jakarta, 6-7 October 2022, 147-152. https://doi.org/10.23919/eecsi56542.2022.9946593

[9] Angraini, Alinda Alias, R. and Okfalisa, O. (2019) Need for Compliance with Information Security Policy in Universities: A Preliminary Survey. 2019 *Fourth International Conference on Informatics and Computing* (*ICIC*), Semarang, 16-17 October 2019, 1-6. https://doi.org/10.1109/icic47613.2019.8985949

[10] Mohammed, A., Kumar, S., Mu'Azu, H.G., Kumar, R., Shah, P., Memoria, M., *et al.* (2022) Data Security and Protection: A Mechanism for Managing Data Theft and Cybercrime in Online Platforms of Educational Institutions. 2022 *International Conference on Machine Learning, Big Data, Cloud and Parallel Computing* (*COM-IT-CON*), Faridabad, 26-27 May 2022, 758-761. https://doi.org/10.1109/com-it-con54601.2022.9850702

[11] Almubayedh, D., khalis, M.A., Alazman, G., Alabdali, M., Al-Refai, R. and Nagy, N. (2018) Security Related Issues in Saudi Arabia Small Organizations: A Saudi Case Study. 2018 21*st Saudi Computer Society National Computer Conference* (*NCC*), Riyadh, 25-26 April 2018, 1-6. https://doi.org/10.1109/ncg.2018.8593058

[12] Zhang, J., Yuan, W. and Qi, W. (2011) Research on Security Management and Control System of Information System in IT Governance. 2011 *International Conference on Computer Science and Service System* (*CSSS*), Nanjing, 27-29 June 2011, 668-673. https://doi.org/10.1109/csss.2011.5974703

[13] Jin, J. and Shen, M. (2012) Analysis of Security Models Based on Multilevel Security Policy. 2012 *International Conference on Management of e-Commerce and e-Government*, Beijing, 20-21 October 2012, 95-97. https://doi.org/10.1109/icmecg.2012.72

[14] Musa, N. (2018) A Conceptual Framework of IT Security Governance and Internal Controls. 2018 *Cyber Resilience Conference* (*CRC*), Putrajaya, 13-15 November 2018, 1-4. https://doi.org/10.1109/cr.2018.8626831

[15] Yang, J. and Jeong, J.P. (2018) An Automata-Based Security Policy Translation for Network Security Functions. 2018 *International Conference on Information and Communication Technology Convergence* (*ICTC*), Jeju, 17-19 October 2018, 268-272. https://doi.org/10.1109/ictc.2018.8539702

[16] Lingga, P., Kim, J., Bartolome, J.D.I. and Jeong, J. (2021) Automatic Data Model Mapper for Security Policy Translation in Interface to Network Security Functions Framework. 2021 *International Conference on Information and Communication Technology Convergence* (*ICTC*), Jeju Island, 20-22 October 2021, 882-887. https://doi.org/10.1109/ictc52510.2021.9620979

[17] Livshitz, I.I., Lontsikh, P.A., Tatarnikova, L.I., Safonova, O.M. and Kozhukhova, V.V. (2020) Evaluation of It-Security Assurance in a Credit Organization. 2020 *International Conference Quality Management, Transport and Information Security, Information Technologies* (*IT&QM&IS*), Yaroslavl, 7-11 September 2020, 114-118. https://doi.org/10.1109/itqmis51053.2020.9322950

[18] Kalinin, M. and Poltavtseva, M. (2024) Big Data Security Evaluation by Bidirectional Analysis of Access Control Policy. 2024 *International Russian Smart Industry Conference* (*SmartIndustryCon*), Sochi, 25-29 March 2024, 98-103. https://doi.org/10.1109/smartindustrycon61328.2024.10515459

[19] Fatemi Moghaddam, F., Emadinia, T., Wieder, P. and Yahyapour, R. (2018) A Sequence-Based Access Control Framework for Reliable Security Management in Clouds. 2018 *IEEE* 6*th International Conference on Future Internet of Things and Cloud* (*FiCloud*), Barcelona, 6-8 August 2018, 108-113. https://doi.org/10.1109/ficloud.2018.00023

[20] Toyeer-E-Ferdoush, Ghosh, B.K. and Taher, K.A. (2021) Security Policy Based Network Infrastructure for Effective Digital Service. 2021 *International Conference on Information and Communication Technology for Sustainable Development* (*ICICT4SD*), Dhaka, 27-28 February 2021, 136-140. https://doi.org/10.1109/icict4sd50815.2021.9396907