Scientific Research Publishing

Journal of Information Security, 2025, 16(1), 44-69
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Designing a Comprehensive Data Governance Maturity Model for Kenya Ministry of Defence

Gilly Gitahi Gathogo[1], Simon Maina Karume[1], Josphat Karani[2]

[1]School of Mathematics & Computer Science, Cooperative University, Nairobi, Kenya
[2]School of Pure and Applied Sciences, Kirinyaga University, Kirinyaga, Kenya
Email: gillygathogo2496@gmail.com

How to cite this paper: Gathogo, G.G., Karume, S.M. and Karani, J. (2025) Designing a Comprehensive Data Governance Maturity Model for Kenya Ministry of Defence. *Journal of Information Security*, **16**, 44-69.
https://doi.org/10.4236/jis.2025.161002

Received: October 28, 2024
Accepted: November 24, 2024
Published: November 27, 2024

Abstract

The study aimed to develop a customized Data Governance Maturity Model (DGMM) for the Ministry of Defence (MoD) in Kenya to address data governance challenges in military settings. Current frameworks lack specific requirements for the defence industry. The model uses Key Performance Indicators (KPIs) to enhance data governance procedures. Design Science Research guided the study, using qualitative and quantitative methods to gather data from MoD personnel. Major deficiencies were found in data integration, quality control, and adherence to data security regulations. The DGMM helps the MOD improve personnel, procedures, technology, and organizational elements related to data management. The model was tested against ISO/IEC 38500 and recommended for use in other government sectors with similar data governance issues. The DGMM has the potential to enhance data management efficiency, security, and compliance in the MOD and guide further research in military data governance.

Keywords

Data Governance Maturity Model, Maturity Index, Kenya Ministry of Defence, Key Performance Indicators, Data Security Regulations

1. Introduction

1.1. Background to the Study

In the past decade, the volume of data generated globally has exponentially increased [1]. This can be attributed to the widespread availability of high-speed Internet connections, the rise of social media platforms, the Internet of things, e-commerce, big data and other emerging technologies. As the data volumes and complexity grow, an organization has two options: To succumb to information

overload or implement data governance to take advantage of the huge potential of the organization's data [2].

There are different uses of data in an organization. Data are required for reporting purposes, decision-making and providing access to vital facts to enable work processes across business units. Data are central to an organization's capacity to anchor fiscal and strategic plans on valid, accurate and current facts, and are also a vital element in an organization's capacity to meet legal, compliance and risk management requirements. To ensure sound decision-making, data must be treated as an asset within organizations, with sound data governance principles entrenched and employed for data handling from inception to deletion [3].

According to [4], data is no longer just bits of information but can be used to inform policy decisions and play an increasingly important role in economics, politics, sustainable development, and even national security. Data can be a tool for prosperity, but also potentially a weapon against the very own organization, institution, or state if it lands in the wrong hands [2]. As the data stockpile continues to grow exponentially and data exchanges and infrastructures mature, more efforts are needed to ensure equitable, controlled, accountable access to certain types of data.

Establishing thorough best practice guidelines for creating a successful data governance maturity model (DGMM) is the goal of this project [1]. It focuses on studying current frameworks and models from diverse industries in order to methodically evaluate various approaches to data governance. It does this by doing a thorough literature analysis to pinpoint the fundamental ideas, standards, and crucial elements of success that have been incorporated into the most popular data governance maturity models [3].

1.2. Kenyan Ministry of Defence Current Data Governance Challenges

The Kenyan Ministry of Defence (MOD) encounters significant data governance challenges that stem from the unique structure and demands of military operations [5]. According to [6], these challenges include issues with integration and interoperability between various systems, data access restrictions, and difficulties in managing legacy systems. Military data requirements vary widely across the MOD's units, each with specific security protocols and mission-critical needs [7].

As per [8], legacy systems, in particular, pose a substantial hurdle as they are not only outdated but also costly to upgrade and difficult to align with newer technologies. The spread of military operations across diverse and sometimes remote locations further complicates data governance efforts, requiring a robust, adaptable approach to support reliable data management [9].

To address these unique needs, the MOD requires a customized Data Governance Maturity Model (DGMM) tailored to its operational complexities [8] [9]. This model would emphasize secure data handling, ensure confidentiality, and improve collaboration across various defence units and interagency partners. The

DGMM's focus on MOD-specific requirements, such as enhanced data security protocols and secure data-sharing mechanisms, is crucial. By aligning the model with these specific challenges, the DGMM can provide a structured framework that not only optimizes data governance practices within the MOD but also facilitates integration and interoperability, ensuring that military data management supports the MOD's mission-critical functions.

1.3. Statement of the Problem

According to [10], it is projected that by 2024, three-quarters of companies will have implemented numerous data hubs to facilitate essential data sharing and governance. By 2024, half of companies will implement up-to-date data quality solutions to enhance their digital business projects. Although data governance processes have been implemented in various government MCDA in Kenya, the Ministry of Defence is distinguished by its complex and diverse nature. In contrast to many government ministries that concentrate on particular aspects of governance or services, each division in the MOD (Army, Airforce, Navy) functions independently with its own objectives, technologies, and operational focuses. This complex framework poses special obstacles in data regulation, because the breadth and depth of data administration at MOD cover a variety of confidential information, including intelligence reports and military logistics. Furthermore, the necessary cooperation between different agencies, which is crucial to the operations of the Ministry of Defence, presents an additional level of complication that is not typically seen in other governmental organizations. The unique characteristics of the MOD environment underline the necessity for a Data Governance Maturity Model designed specifically to meet the complex requirements of the MOD. This research aimed to create a Data Governance Maturity Model to assess levels of data governance maturity in Kenya's Ministry of Defence.

1.4. Objectives of the Study

The main objective of this study was to develop a Maturity Model that will measure Data Governance Maturity in the Kenya Ministry of Defence. The study was guided by the following specific objectives:

1) To investigate the Key Performance Indicators (KPIs) required for measuring Data Governance Maturity levels in the Kenya Ministry of Defence.

2) To derive a Data Governance Maturity Model (DGMM) model for measuring data governance maturity levels based on the KPIs identified.

3) To implement a prototype model as a web-based tool.

4) To validate the model at the Kenya Ministry of Defence.

1.5. Research Question

To achieve the objective, the study was guided by the following research questions:

1) What are the KPIs required to measure data governance implementation within the Kenya Ministry of Defence?

2) How can the model be derived?
3) How can the DGMM web-based tool be implemented?
4) How can the model be validated?

2. Literature Review

2.1. Data Governance

As per [11], data governance involves overseeing the accessibility, usability, reliability, and protection of data within a company, and has gained more appreciation, particularly in public sector institutions, where transparency and accountability are crucial [12]. Data governance frameworks are crucial for organizations to strategically manage their data assets, ensuring accuracy, consistency, and accessibility, while also protecting sensitive information [13]. Moreover, incorporating data governance into company procedures can boost decision-making and enhance operational efficiency, as noted by Koltay [11].

2.2. Data Governance Maturity Model

The Data Governance Maturity Model (DGMM) provides a structured approach to assess and improve an organization's data governance capabilities [4]. It typically consists of several maturity levels, each representing a stage of development in data governance practices [14]. These levels range from ad-hoc and chaotic processes to optimized and fully integrated governance frameworks [15] [16]. The model serves as a diagnostic tool that enables organizations to identify their current maturity level and develop a roadmap for improvement [14]. Through such models, organizations can benchmark their practices against industry standards and best practices, facilitating continuous improvement in data governance [12].

2.3. Data Governance Maturity Model Key Performance Indicators

Measuring the effectiveness of data governance initiatives is crucial through the use of Key Performance Indicators (KPIs), as they offer measurable metrics to assess progress in implementing data governance practices [17]. According to [18], the key performance indicators commonly found in data governance maturity models are metrics for data quality, compliance rates, user satisfaction levels, and the frequency of data-related incidents [19]. By defining specific KPIs, companies cannot just monitor their progress but also make well-informed choices on where to allocate resources and which strategic path to take in their data governance initiatives [17].

2.4. Data Governance Maturity Model Design

Creating a Data Governance Maturity Model requires defining maturity levels, identifying data governance dimensions, and establishing assessment criteria [16]. The model needs to be customized to fit the organization's unique needs and situation, while considering factors like organizational culture, regulations, and

current data practices [5]. An effectively developed maturity model not only assists in self-evaluation but also motivates companies to embrace optimal methods and harmonize their data governance plans with their broader business goals [17].

2.5. Kenya Ministry of Defence Operating Environment

The Kenya Ministry of Defence (MoD) faces complex data management challenges, such as ensuring secure data sharing, complying with strict regulations, and incorporating various data sources [5]. The Kenya MoD's framework for data governance needs to tackle these obstacles, ensuring data is available to authorized users and safeguarded from unauthorized access [6]. Moreover, the ever-changing aspect of defence operations requires an adaptable and reactive data governance strategy that can adjust to changing threats and operational needs [20].

2.6. Data Governance Maturity Evaluation Model (DGMEM)

The DGMEM is a framework created explicitly to evaluate how mature data governance practices are in a company [19]. Usually, it consists of a series of standards and measures that companies can utilize to assess their existing situation and pinpoint opportunities for enhancement [17]. The DGMEM aids in gaining a thorough grasp of an organization's data governance capabilities, allowing stakeholders to make well-informed decisions regarding needed improvements and allocation of resources. By using the DGMEM, companies can strategically improve their data governance maturity and better align with strategic objectives.

2.7. Research Gap

While there is an increasing amount of research on data governance and maturity models, there is still a notable gap in the literature regarding how these models are specifically applied within the Kenya Ministry of Defence. The majority of current research concentrates on generic models without acknowledging the specific obstacles and needs encountered by defence agencies [20].

Furthermore, there is a shortage of research studies that assess how data governance maturity models can improve operational efficiency and decision-making in military situations [6]. This opening allows for additional research to create customized data governance frameworks that support the strategic goals of the MoD in Kenya.

2.8. Conceptual Framework

The study was guided by the conceptual framework shown in **Figure 1** below. The formula for calculating the Data Governance Maturity Index was determined as a function of measurable People KPIs, Processes KPIs, Technology KPIs, and Organization KPIs that were identified. The specific mathematical expression for deriving this formula is as shown below:

$$\text{DGMI} = f\left(\text{KPIs Identified}\right). \tag{1}$$

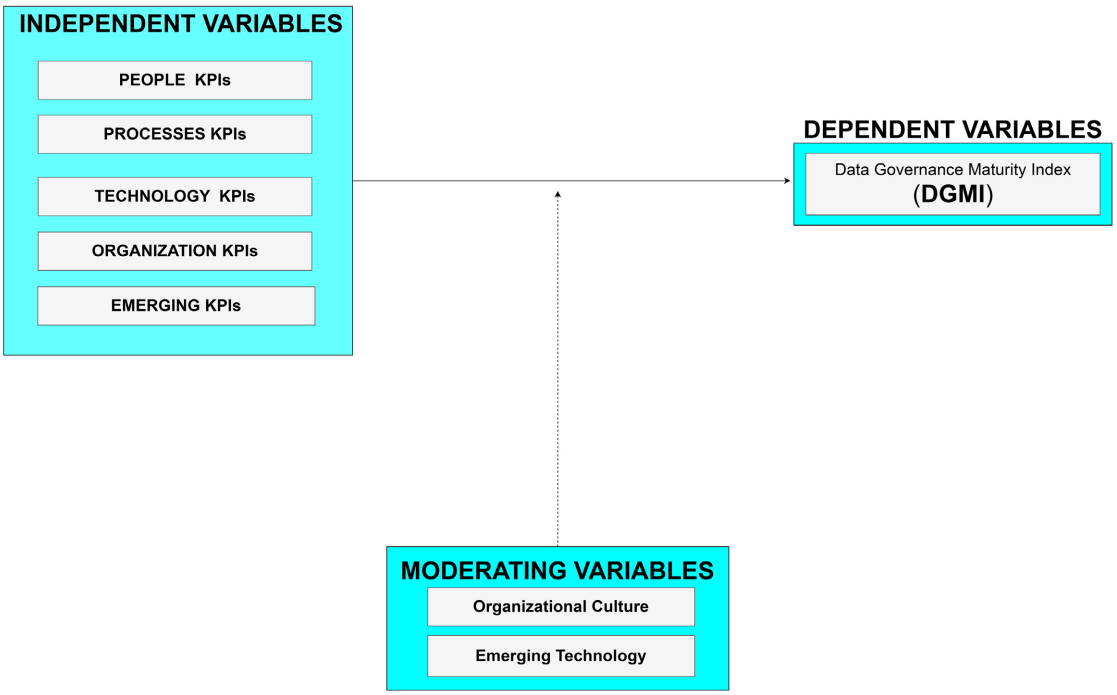

Figure 1. The conceptual framework for the study.

The classification of independent variables was driven by the unique challenges and requirements inherent in the MOD's data governance landscape. This study evaluated People to identify and validate the critical human components required in implementing a successful data governance Maturity Model in a military context. Processes were critical in reviewing internal procedures, while technology concentrated on assessing the deployment of modern Data Governance solutions customized to the MOD's complex data ecosystem.

Organizational KPIs focus on the defence organization's hierarchical and functional characteristics. Furthermore, Emerging KPIs account for the ever-changing technology landscape. This classification distinguished this study by giving a specialized methodology that incorporated specific complexities of the MOD's data governance requirements, providing a complete and contextualized methodology for maturity assessment that is not found in generic data governance maturity models.

2.9. Impact of DGMM on National Policy

The development of a Data Governance Maturity Model (DGMM) for the Kenyan Ministry of Defence (MoD) has the potential to significantly shape national data governance policies by establishing a robust standard for managing sensitive data within government sectors [21]. By specifically addressing the unique needs of the defence sector, the DGMM can offer a structured framework that other sensitive government departments, such as education, health, and finance, could adopt or adapt.

This model's emphasis on security, accountability, and efficient data management

in high-stakes environments could serve as a benchmark, encouraging consistency and rigor in data handling practices across Kenya's public sector. As a result, the DGMM could be instrumental in promoting a culture of transparency [17] [18], trust, and heightened data stewardship in national institutions handling sensitive information [21].

Aligning the DGMM with established regulatory frameworks such as Kenya's Data Protection Act (DPA) [9] and international standards like the General Data Protection Regulation (GDPR) [22] [23] further enhances its impact. The DGMM's incorporation of these frameworks ensures that its data governance recommendations support privacy rights, data security, and compliance, which are critical for both national and international partnerships [21].

Through harmonizing with the DPA and GDPR, the DGMM could streamline regulatory practices, reduce compliance burdens, and create a coherent, adaptable model that can be scaled across various government entities [17]. This alignment not only strengthens Kenya's data governance infrastructure but also reinforces Kenya's position in global data privacy and security initiatives, making it a valuable reference for policymakers looking to refine data governance laws and improve regulatory oversight in other sectors.

3. Methodology

3.1. Research Design

This research utilized Design Science Research as its research design to direct the study. It is a research methodology focused on creating and assessing new products to improve the surroundings [24]. It promotes thought, education, and adjustment during the study, providing a systematic approach to developing creative answers to intricate real-life issues [25]. Research design plays a crucial role in connecting research questions with methods, as stated by [26]. It is a comprehensive summary of the research methodology.

Through the utilization of Design Science Research, the research project developed, constructed, and assessed the Data Governance Maturity Model in a methodical way, guaranteeing its harmony with the ever-changing landscape of Data Governance in the Kenya MOD. This not only addressed Kenya MOD's specific needs and challenges but also added value to the wider Data Governance field.

3.1.1. Data Collection

This study employed a mixed-method approach [27], combining quantitative and qualitative research methods to thoroughly explore data governance practices within the Ministry of Defence (MoD). According to [25], quantitative methods, particularly surveys, were used to capture structured, measurable data regarding current data governance maturity levels across various units within the MoD.

These surveys provide statistical insights that reveal patterns, trends, and the overall state of data governance practices [28] [29]. By quantifying specific aspects, such as compliance levels, data management capabilities, and technical resources,

the quantitative data offer an objective baseline that can be analyzed to identify gaps and areas for improvement in the MoD's data governance framework.

In parallel, qualitative methods, notably interviews with data management experts and MoD personnel, offer deeper [30], contextually rich insights into the challenges and nuances of data governance within the military environment. These interviews provide detailed narratives and perspectives on issues like data integration, security requirements, and practical obstacles in implementing governance policies across different branches.

The qualitative data illuminate the lived experiences of those directly involved in data management, capturing insights that quantitative data alone might overlook [27] [31]. By combining both methods, the study achieved a comprehensive view of the MoD's data governance landscape, ensuring that the proposed Data Governance Maturity Model (DGMM) addresses both statistical needs and the practical realities within the organization.

3.1.2. Sampling Technique and Sample Size

This research used a purposive sampling method, targeting individuals with considerable experience and knowledge in data management practices in the Kenya MOD. The reason for the choice of the approach was based on the core principles of DSR, which highlight the significance of engaging domain experts with a deep understanding of the problem domain [32].

This guaranteed that the created Data Governance Maturity Model would be based on practical knowledge and would suit the specific requirements and difficulties encountered by the Kenya MOD. Due to the scarce data management personnel in Kenya MOD and the researchers' desire to thoroughly comprehend the experiences, perceptions, opinions, feelings, and knowledge of each individual, the study conducted interviews and surveys with all 162 personnel in this group, thus ensuring a complete and detailed analysis.

3.2. Model Development

In order to calculate the DGMI, the research included data governance elements organized into People, Processes, Technology, Organizational, and Emerging factors, along with moderating factors like organizational culture and emerging technologies. Factors will be described in the following steps:

1) *People Factors* (*PF*): KPIs related to human resources, skills, and roles in data governance.

2) *Process Factors* (*PrF*): KPIs related to data management processes, workflows, and governance procedures.

3) *Technology Factors* (*TF*): KPIs related to data infrastructure, tools, and technologies supporting data governance.

4) *Organizational Factors* (*OF*): KPIs related to organizational structures, policies, and strategies impacting data governance.

5) *Emerging Factors* (*EF*): KPIs related to emerging trends, challenges, and opportunities affecting data governance.

6) *Organizational Culture* (*OC*): A moderating variable representing the organizational values, norms, and behaviors influencing data governance effectiveness.

7) *Emerging Technologies* (*ET*): A moderating variable representing the impact of new technologies on data governance practices.

By applying Principal Component Analysis (PCA), factor scores were calculated for every data point, considering their answers to the Key Performance Indicators (KPIs) in each factor. Factor scores indicate the significance or impact of each individual observation. Factor scores were adjusted to ensure consistency across observations. PCA was used to determine weights based on data gathered on current data governance practices at the MOD. These weights represented the significance and influence of each KPI towards the overall maturity of data governance.

- P = Weight assigned to People factors
- Pr = Weight assigned to Processes factors
- T =Weight assigned to Technology factors
- O = Weight assigned to Organizational factors
- E = Weight assigned to Emerging factors
- C = Weight assigned to Organizational Culture (Moderating Variable)
- ET = Weight assigned to Emerging Technologies (Moderating Variable)
- For each observation i

The Data Governance Maturity Index was computed as follows:

$$\text{DGMI} = \sum_{i=1}^{n} \left(\text{FactorWeightages}_i \times \text{FactorScore}_i \right) \quad (2)$$

In general, the model calculated the Data Governance Maturity Index (DGMI) by comparing the MOD existing data governance status to the ISO/IEC 38500 best practice benchmarks. If the results fall below the stated threshold, notifications will be produced, emphasizing specific Key Performance Indicator (KPI) gaps that must be addressed.

3.3. Construction Process of DGMM

The construction process of the Data Governance Maturity Model (DGMM) for the Kenyan Ministry of Defence (MoD) encompassed several essential stages, utilizing a methodical approach to design principles, performance indicators, and model-specific features. The construction followed the following three steps.

3.3.1. Model Design Principles

The model was developed based on the Design Science Research (DSR) methodology, which facilitated an iterative cycle of design, feedback, and modification to address complex, real-world challenges effectively. This iterative method enabled the study to meet the unique requirements of the military environment, focusing specifically on secure data management and adaptable frameworks to handle evolving operational needs.

To ensure alignment with recognized standards, the DGMM was benchmarked

against ISO/IEC 38500 and CMMI standards. These benchmarks helped integrate best practices in data governance, allowing the MoD to progress from basic awareness of data governance needs to fully optimized and integrated processes as represented by maturity levels ranging from "Unaware" to "Mature."

3.3.2. Selected Key Performance Indicators

Key performance indicators (KPIs) formed an essential component of the DGMM, derived from core data governance areas grouped into categories: People, Processes, Technology, Organizational, and Emerging Factors. Each category encompassed specific KPIs tailored to address the MoD's requirements. For example, the "People Factors" category included KPIs related to skills, roles, and responsibilities within data governance. The "Process Factors" assessed workflows, data management processes, and compliance practices.

"Technology Factors" evaluated the application of data infrastructure and governance-supportive technologies, while "Organizational Factors" focused on policies and structures influencing data governance. Finally, "Emerging Factors" addressed the integration of new technologies to keep up with evolving demands. Additional KPIs were incorporated to ensure responsiveness to defence-specific requirements, including areas such as Data Quality, Data Security, AI and Analytics, Data Privacy, Data Accuracy, and Meta Data Management. These KPIs were selected for their relevance to maintaining data integrity, accuracy, and operational compliance in a high-security environment.

3.3.3. Mathematical Modeling for DGMI

Mathematical modeling for the DGMM involved the development of a Data Governance Maturity Index (DGMI), using a weighted linear regression approach to calculate maturity scores for each KPI. Weights for each KPI were assigned through Principal Component Analysis (PCA), which helped accurately capture the MoD's distinct data governance landscape. The DGMI applied these scores to categorize the MoD's maturity level on a scale from 0 to 100%, with 0% indicating no governance integration (Level 1) and 100% representing full integration and optimization (Level 6). The summary of the construction process of DGMM is shown in Figure 2 below.

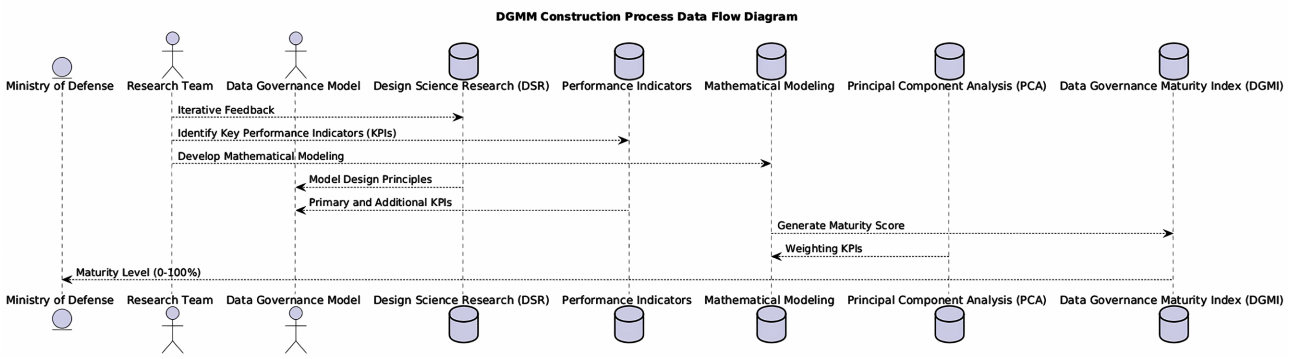

Figure 2. Construction process of DGMM.

4. Results and Discussions

4.1. Return Rate

During the data collection process, questionnaires were distributed to 115 respondents within the ministry. Out of these, 105 completed the questionnaires, yielding a response rate of 91.3%. The completed questionnaires were considered adequate to provide the necessary data for the study.

4.2. Respondents Basic Information

This subsection gives a summary of the respondents' personal data, such as their job titles and work history, which helped put the study's conclusions in perspective.

Table 1. Distribution of positions held.

S/NO	Role	Freq	Percentage (%)
1.	IT Officers	24	22.9
2.	SOC Analysis	10	9.5
3.	Digital Forensics	10	9.5
4.	Hub	9	8.6
5.	Data Center Engineers/Tech	11	10.5
6.	Other Roles: (Cyber, Network, IR, Admin)	41	39

From Table 1 above, the analysis indicated that a significant portion of the respondents hold positions related to data governance. Combined, these roles represent approximately 52.4% of the total respondents (IT Offices, SOC Analysis, Digital Forensics and Data Center Engineers/Tech), thereby constituting the majority. This distribution suggests that the selected respondents are well-positioned to provide relevant insights for the study as their roles involve key responsibilities and expertise in managing, securing, and overseeing data-related functions within the Kenya Ministry of Defence.

4.3. Years of Experience in Current Positions

Analysis of the years of experience vis-à-vis the positions held by the respondents, the findings were as follows:

- **IT Officers**. Out of 24 IT Officers, 46% had 4 - 7 years of experience, while 33% had 8 - 14 years, indicating a mix of mid-level and senior professionals in this role.
- **SOC Analysts**. Half of the SOC Analysts (50%) had 4 - 7 years of experience, showing a balanced mix of mid-career professionals, with 30% having 8 - 14 years of expertise.
- **Digital Forensics Analysts**. 50% of the Digital Forensics Analysts possessed 8 - 14 years of experience, reflecting a high level of seniority within this group.

- **StratCom and Hub Roles**. Nearly 45% of StratCom personnel had 4 - 7 years of experience, while 33% had 8 - 14 years, showing a diverse range of experience levels.
- **Data Center Personnel**. The experience was evenly split between those with 4 - 7 years and 8 - 14 years (45.5% each), suggesting a well-distributed level of expertise across the team.

4.4. Awareness and Perceptions

Three main questions were posed about respondents' knowledge of the standards and policies controlling MOD data management during its lifetime, the efficacy of these policies, and the clarity of the reporting frameworks for data governance issues. The answers, as summarized in Table 2 below, were meant to shed light on how well-understood and successful data governance is at MOD.

Table 2. Awareness and perceptions.

S/No	Aspect	Yes (%)	No/Uncertain (%)
1.	Awareness of policies and Standards	100%	0%
2.	Believe in Data Governance	87%	13%
3.	Existence of clear reporting structures for accountability	94%	6%

From Table 2 above, these percentages demonstrate that the majority of participants have a strong understanding and involvement in data governance. This aligns with the research mission to evaluate data governance maturity within the MOD, indicating that the selected respondents possessed the necessary insights and experiences to effectively contribute to the study.

4.5. Descriptive Findings

In order to achieve objective one, the respondents were asked to rate their level of satisfaction with the Data Governance KPIs on a scale of 1 to 5, with 1 denoting extreme dissatisfaction and 5 denoting extreme satisfaction, in response to the assessment question. Likewise, the remaining answers were Satisfied, Neutral, and Dissatisfied. The degree of Data Governance was indicated by the respondents' ratings for each assessment question.

Table 3. Level of satisfaction with the data governance KPIs.

S/no	FACTOR	Very Dissatisfied	Dissatisfied	Neutral	Satisfied	Very Satisfied	Total Score	% Score
1.	Data Quality	0	1	7	18	79	490	93.33%
2.	Data Management	0	0	13	11	17	468	92.67%
3.	Data Security	0	4	12	21	65	453	88.82%

From Table 3 above, Data Security (88.82%) was shown to perform poorly, whereas Data Management (92.67%) and Data Quality (93.33%) showed excellent

performance. The findings showed excellent performance in terms of data management and quality, which suggested efficient procedures for the production and use of data. That being said, the lower security rating indicated flaws in later phases, such as data storage and disposal, hence underscoring the necessity of a maturity model that would provide equal attention throughout the data lifecycle, guaranteeing that data protection measures are sustained throughout all phases from creation to disposal.

4.6. Factor Analysis

To facilitate multivariate analysis and improve interpretability, the variables were coded as shown in Table 4 below:

Table 4. Variables used in the study.

Code	Variable	Meaning
DQ	Data Quality	Ensuring the data is accurate, consistent, and reliable.
DM	Data Management	Managing data from creation to disposal effectively.
DS	Data Security	Safeguarding data against unauthorized access and breaches.
DP	Data Privacy	Ensuring compliance with data privacy laws and regulations.
DST	Data Stewardship	Assigning roles for responsible data oversight.
DA	Data Architecture	Structuring and managing data storage, retrieval, and organization.
DPS	Data Policies & Standards	Enforcing policies and standards across the data lifecycle.
MD	Meta Data Management	Handling metadata to improve data discovery and context.
DAC	Data Accuracy	Maintaining correctness and precision of data.
SE	Strict Enforcement	Implementing strict governance enforcement policies.
DE	Data Encryption	Using encryption methods to protect data.
MFA	Multifactor	Securing data with additional authentication layers.
DGT	Data Gov Team	Ensuring that a dedicated team governs data-related policies.
RS	Reporting Structure	Defining the structure for data reporting and accountability.
AI	AI Analytics	Leveraging artificial intelligence for data analysis and insights.
DO	Data Officer	Designating roles responsible for data governance compliance

4.7. Principal Component Analysis

Principal Component Analysis (PCA) was used as the extraction method, with two components being extracted. The purpose of PCA is to reduce the dimensionality

of the dataset by identifying variables that explain most of the variance. The Scree Plot helped visualize how many components are necessary before diminishing returns on variance explanation as observed.

4.8. Total Variance

The Total Variance explained by the two components was significant. The first component explained the majority of the variance (4.123), while subsequent components explained much less variance.

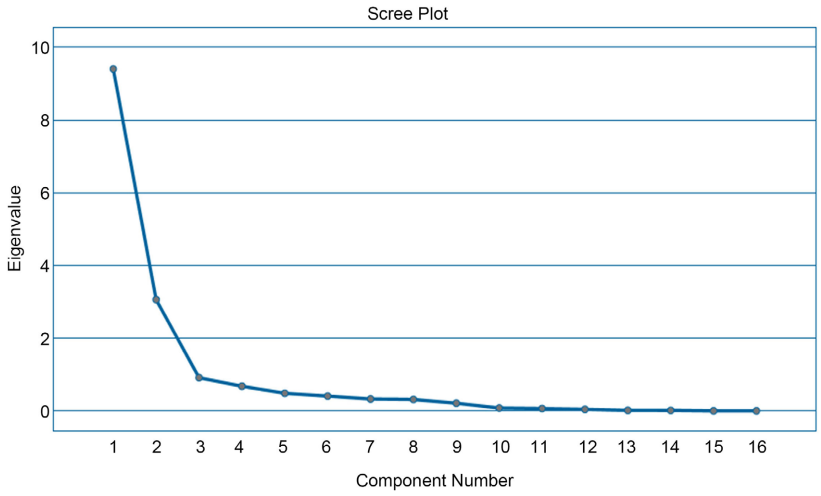

Figure 3. Scree plot from factor analysis.

The scree plot from Figure 3 above indicated that the first component is dominant, suggesting a strong influence of core governance factors such as security, quality, and accuracy.

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	9.402	58.761	58.761	9.402	58.761	58.761	8.041
2	3.058	19.111	77.872	3.058	19.111	77.872	6.988
3	.914	5.711	83.584				
4	.677	4.231	87.815				
5	.482	3.012	90.827				
6	.406	2.536	93.362				
7	.326	2.039	95.401				
8	.315	1.967	97.368				
9	.210	1.315	98.683				
10	.079	.493	99.176				
11	.064	.401	99.577				
12	.042	.262	99.839				
13	.013	.083	99.922				
14	.013	.078	100.000				
15	-2.859E-15	-1.787E-14	100.000				
16	-6.313E-15	-3.945E-14	100.000				

Figure 4. Total variance.

Figure 4 above suggests that most of the data governance variables are closely related and could be summarized by these key components.

4.9. Communalities

Communality values represented the amount of variance in each variable accounted for by the extracted factors, as indicated in Figure 5 below.

	Initial	Extraction
DQ	1.000	.783
DM	1.000	.877
DS	1.000	.658
DP	1.000	.578
DST	1.000	.738
DA	1.000	.779
DPS	1.000	.860
MD	1.000	.841
DAC	1.000	.811
SE	1.000	.913
DE	1.000	.688
MFA	1.000	.816
DGT	1.000	.524
RS	1.000	.792
AI	1.000	.930
DO	1.000	.871

Figure 5. Communalities.

4.10. Factor Loadings

Factor loadings provided insight into how strongly each variable is associated with the extracted components. Variables with high loadings on a given factor are more strongly related to that component. The findings are as follows:

1) AI Analytics (AI) and Meta Data Management (MD) had high loadings, suggesting these are crucial elements of the maturity model.

2) Data Security (DS) and Data Accuracy (DAC) also showed significance, although their loadings were slightly lower, indicating moderate contributions.

4.11. Reproduced Covariance Matrix

The reproduced covariance matrix showed the covariance between variables after accounting for the factors extracted. Covariances between key variables like AI Analytics, Data Quality, and Meta Data Management were strong, underscoring their interconnectedness.

4.12. Component Correlation Matrix

The component correlation matrix revealed how closely the two extracted factors are related. A high correlation indicated that the factors shared a substantial amount of information, suggesting that variables like Data Security, AI, and data quality are not entirely independent but work together in forming a comprehensive governance structure.

The component correlation matrix revealed how closely the two extracted factors are related. The figure below represents the Component Correlation Matrix from a principal component analysis (PCA) with oblique rotation (Oblimin with Kaiser Normalization). From the findings in Figure 6 below, Diagonal values (1.000) indicated that each component correlates perfectly with itself, while Off-diagonal value (0.412) indicated a moderate positive correlation between the two components. It is indicated that the variables are related but still have some distinctiveness.

Component	1	2
1	1.000	.412
2	.412	1.000

Figure 6. Component correlation matrix.

4.13. Interpretation of Key Variables

4.13.1. Significance of Variables

- **Data Security (DS):** Moderate communalities and factor loadings indicated that while important, it may not be the primary driver in the model. However, given the nature of the ministry, inclusion remains essential.
- **Data Quality (DQ):** Moderate communalities suggested it is important, but not as dominant as some other variables.
- **AI Analytics (AI):** Strong communalities and loadings indicated that AI should be a central feature of the data governance maturity model, reflecting the increasing role of AI in data management.
- **Meta Data Management (MD):** High communalities and loadings imply that effective metadata management is crucial for achieving a high level of maturity.
- **Data Accuracy (DAC) and DO:** Moderate significance suggested that while not a primary driver, accuracy is essential for ensuring the reliability of the data governance structure.

4.13.2. Highly Correlated Variables

The below variables exhibited high correlation with each other as shown below:

- DQ and DM (0.855).
- DS and DP (0.842).
- AI and DO (0.921).

This suggested that the variables possibly had similar underlying attributes, which presented an opportunity to select one representative variable from each pair where applicable in order to avoid redundancy in the model.

4.13.3. Key Contributors from Component Analysis

Going by the result from the Component Score Coefficient Matrix:

- **Component 1:** DM, DPS, MD had higher coefficients, indicating they are significant contributors to this component.
- **Component 2:** DAC, DE, and MFA had higher coefficients, making them

important for understanding this component.

4.13.4. Variables with Moderate Correlation across Components

AI, DE, and DO exhibit more balanced correlations across different components and hence useful in capturing a variety of dimensions and providing a comprehensive model.

4.13.5. Variables with Lower Correlations

RE, SE and DGT had lower or negative correlations. However, in order to capture the unique aspects that are not explained by other variables, including them could add valuable diversity.

4.14. Principal Component Analysis (PCA) and Communalities

The factor analysis using PCA extracted two components, which explained a substantial portion of the variance. From the extraction method used, the communalities such as Data Security (DS) = 0.902, Data Quality (DQ) = 0.921, AI = 0.935, Meta Data Management (MD) = 0.769, Data Accuracy (DA) = 0.824) indicated how much of the variance in each variable is explained by the extracted factors.

- **Data Security (DS):** With a communality of 0.902, it suggested that most of the variance in Data Security is captured by the components, highlighting its importance in the model.
- **Data Quality (DQ):** A communality of 0.921 showed that it is a highly significant variable, and thus plays a critical role in the overall data governance model.
- **AI Analytics:** With a communality of 0.935, this indicated that AI contributes significantly to the variance explained by the components. AI is integral to advanced data analytics and governance frameworks.
- **Meta Data Management (MD):** Its communality of 0.769 also showed significance, though slightly lower than DS, DQ, and AI. Nevertheless, metadata management is crucial for ensuring the usability and traceability of data.
- **Data Accuracy (DAC):** The communality of 0.824 highlighted its importance.

A summary of the selected variables from the KPIs for the model development is shown in Table 5 below.

Table 5. Summary of variables selected for the model.

Category	Selected Variables (KPIs)	Justification
Primary Variables	Data Policies (DPS), Data Accuracy (DAC), Data Encryption (DE), Multi-Factor Authentication (MFA).	Significantly loaded on components and cover different dimensions.
Distinct Elements	Strict Enforcement (SE), Reporting Structure (RS), Data Governance Team/Office (DGT)	To include unique elements not covered by primary variables.
From Highly Correlated Pairs	Data Management (DM), Data Security (DS), Artificial Intelligence & Analytics (AI)	Chosen from pairs to avoid multicollinearity.

4.15. Derivation of DGMI Mathematical Model

A Linear Regression Analysis was conducted in order to compute variable weights necessary for the derivation of the mathematical model, as shown in Figure 7 below.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95.0% Confidence Interval for B		Correlations			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	1.599E-14	.000		.	.	.000	.000					
	DQ	1.000	.000	.163	.	.	1.000	1.000	.909	1.000	.064	.154	6.486
	DM	1.000	.000	.183	.	.	1.000	1.000	.901	1.000	.085	.217	4.615
	DS	1.000	.000	.212	.	.	1.000	1.000	.851	1.000	.130	.373	2.682
	MD	1.000	.000	.225	.	.	1.000	1.000	.854	1.000	.109	.236	4.238
	DAC	1.000	.000	.117	.	.	1.000	1.000	.739	1.000	.058	.241	4.144
	AI	1.000	.000	.138	.	.	1.000	1.000	.896	1.000	.040	.084	11.972
	DO	1.000	.000	.131	.	.	1.000	1.000	.797	1.000	.039	.087	11.440

a. Dependent Variable: DGMI

Figure 7. Regression coefficients.

Given that all the unstandardized coefficients (β) for the independent variables are equal to 1.000, the formula simplifies significantly.

$$\text{DGMI} = \beta_0 + \beta_1\text{DQ} + \beta_2\text{DM} + \beta_3\text{DS} + \beta_4\text{MD} + \beta_5\text{DAC} + \beta_6\text{AI} + \beta_7\text{DO} \quad (3)$$

Since all coefficients are constant (1.000), then

$$\text{DGMI} = \beta_0 + \text{DQ} + \text{DM} + \text{DS} + \text{MD} + \text{DAC} + \text{AI} + \text{DO} \quad (4)$$

Therefore, DGMI = $\beta_0 + \beta_1 \cdot V_1 + \beta_2 \cdot V_2 + \beta_3 \cdot V_3 + \ldots + \beta_n$. X_n for n variables. where:

β_0: is the constant term (intercept), which is 1.599×10^{-14};

β_1: are the coefficients for each variable, all set to 1.000;

V: is the independent variable.

To assign maturity level scores, the study used the Hybrid Maturity level Model as shown in Table 6 below, which was derived from the CMMI and Gartner Maturity Model; and benchmarking the guiding principles of ISO 38500.

Table 6. Hybrid maturity level model.

Maturity Level	Description	Score (X)
Unaware/None	No formal governance processes.	0
Aware	Basic recognition of governance needs.	1
Defined	Formal processes are in place, but not standardized.	2
Managed	Processes are managed, measured, and controlled.	3
Optimized	Processes are continuously improved based on metrics.	4
Mature	Fully integrated Data governance and continuous improvement.	5

The following linear regression modeling equation was used to compute weights necessary for computing the Maturity Index Y, in this case, the Data Governance Maturity Index (DGMI).

$$Y = W_1V_1 + W_2V_2 + \cdots W_nV_n \tag{4}$$

where,

Y = Data Governance Maturity Index (MI);

W = Weights;

V = Data Governance Key Performance Indicators (KPIs)/(User assessment Score per question);

n = Number of assessment questions.

Assuming that the coefficients of the assessment questions are constant,

Thus $W = W_1 = W_2 = \ldots W$, Consequently, W will be the weight, thus

$$MI = WV_1 + WV_2 + WV_3 \cdots WV_n \tag{5}$$

Since W is common

$$MI = W\left(V_1 + V_2 + V_3 \cdots V_n\right) \tag{6}$$

This study had 16 questions that directly assessed the Data Governance KPIs (Variables), but after factor analysis, 10 KPIs were selected; therefore, case, $n = 10$ and the maximum score that the user could have on a scale of 1 to 5 was $5 \times 10 = 50$.

Putting this back into the previous equation, then

$$\text{MI} = V_1/50 + V_2/50 + V_3/50 + \cdots V_{1O}/50 \tag{7}$$

Therefore,

$$\text{MI} = 1/50\left(V_1 + V_{12} + V_{31} + \cdots V_{10}\right) \tag{8}$$

Hence $W = 1/50 = 0.002$.

The relevant weight for the DGMI model was 0.002, as shown in the results above.

To compute the MI as a percentage factor,

$$\text{MI} = 0.02\left(V_1 + V_{12} + V_{31} + \cdots V_{10}\right) \times 100 \tag{9}$$

Percentage Maturity Index

Achieving a specific Maturity Index indicates the organization's overall posture and the percentage of Data Governance maturity it represents. Below is the equation for computing Data Governance Maturity Index (DGMI).

$$\text{DGMI} = \text{MI}\% \tag{10}$$

4.16. Model Scenarios

Below demonstrations depict the three model scenarios.

- **Best Case Scenario:** Full score (DGMI = 100%), indicating complete governance integration.
- **Average Case Scenario:** Mid-level score (DGMI = 50%), suggesting a moderate level of governance maturity.

- **Worst Case Scenario:** Minimum score (DGMI = 20%), highlighting significant governance deficits.

Table 7 below is a summary of the maturity thresholds and the assessment scale.

Table 7. Maturity thresholds.

Level	Maturity Level	Score	DGMI (%)	Description
Level 1	Unaware	0	0%	Organization has no formal data governance.
Level 2	Aware	1	20%	Basic awareness of data governance exists.
Level 3	Defined	2	40%	Data governance processes are defined but not fully operational.
Level 4	Managed	3	60%	Data governance processes are actively managed and followed.
Level 5	Optimized	4	80%	Processes are optimized for efficiency and effectiveness.
Level 6	Mature	5	100%	Data governance is fully integrated and continually improved.

4.17. Assessment Scale

From Figure 8 below, a range of scores from 0 to 80, or percentages from 0% to 100%, are depicted by the DGMI scale below.

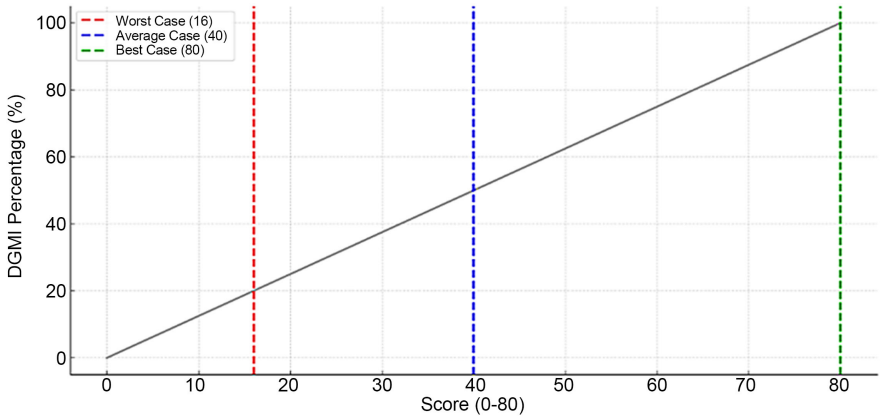

Figure 8. Maturity assessment scale.

The green zone denotes a mature Data Governance program, the blue zone represents an average level of implementation, and the red zone signifies a critical stage where the program needs immediate attention and corrective action.

5. Model Implementation

5.1. Model Implementation Summary

The Data Governance Maturity Model (DGMM) prototype was implemented to provide a structured tool for assessing the maturity of data governance practices within the Kenya Ministry of Defence (MOD) and potentially other government agencies. The system was developed using Python Django, MySQL for database

management, and front-end styling with CSS3 and JQuery for interactivity. The model includes modules for user authentication, data entry, maturity assessment, insights generation, and report download, ensuring comprehensive functionality and security. Key participants include users and administrators, who manage and interact with the system to assess and enhance data governance maturity. A rapid prototyping approach was used, incorporating requirements gathering, quick design, coding, evaluation, testing, and deployment phases.

5.2. System Architecture and Modules

The DGMM system architecture integrates essential components like user authentication, session handling, and a maturity assessment module. Users input data through a Likert scale interface, and the system calculates a maturity index based on predefined Key Performance Indicators (KPIs). Results are displayed in a user-friendly format with insights on improving data governance practices. The system's core modules include a user registration and password management module, a database with assessment questions, as shown in Figure 9 below, and an insights module that generates targeted recommendations based on assessment scores shown in Figure 10 below.

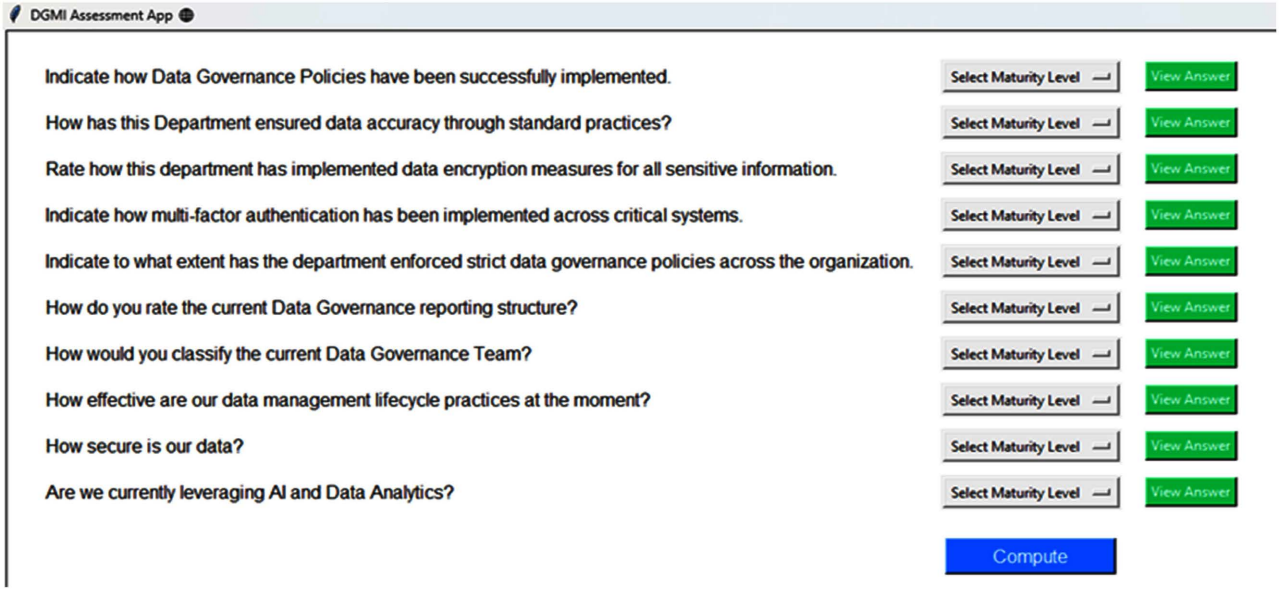

Figure 9. Module of the system on assessment questions.

Figure 10. The output assessment scores.

5.3. Prototype Evaluation

The prototype was evaluated using the FEDS approach to ensure alignment with system objectives. It successfully validated user registration, authentication, DGMI assessment, and logic computation, meeting all intended functionality requirements. The insights module displayed assessment results, as shown in Figure 11 and Figure 12 below and allowed users to download them as a PDF, demonstrating effective, user-centric features for real-world application.

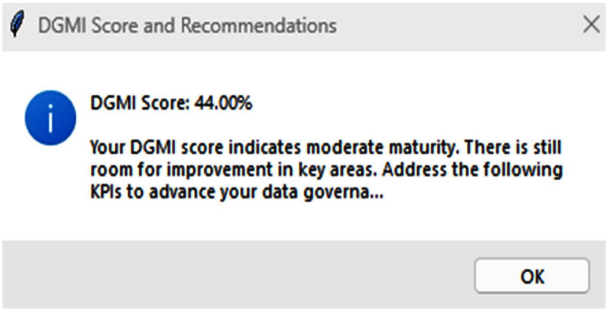

Figure 11. DGMI score and recommendations.

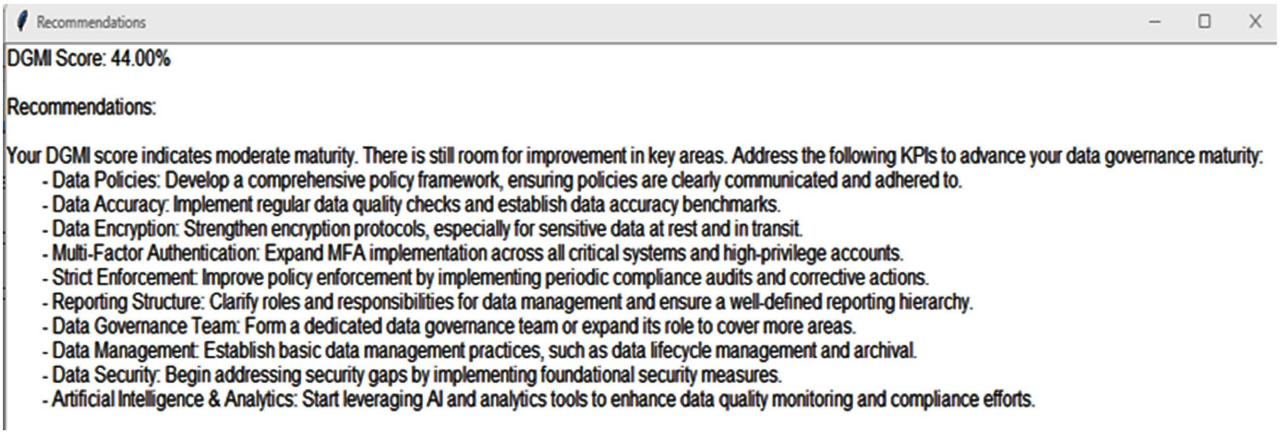

Figure 12. DGMI Recommendations.

6. Conclusions and Recommendations

6.1. Conclusions

The study effectively developed a Data Governance Maturity Model (DGMM) tailored for the Kenya Ministry of Defence (MOD), providing a robust tool for assessing and enhancing data governance practices. By addressing the gaps in current methodologies, this DGMM facilitates systematic maturity evaluation, offering insights crucial for guiding improvements in data governance, security, and management. The model's applicability extends beyond the MOD, serving as a valuable resource for other government ministries, and agencies (MDAs) aiming to strengthen their data governance frameworks. Through rigorous validation, the DGMM model proved reliable in delivering accurate and actionable insights for data governance maturity.

6.2. Recommendations

It is recommended that the DGMM model be incorporated as an integral part of the Kenya MOD's audit processes alongside other auditing tools used across government MDAs. This integration will enhance the ministry's data governance capabilities by providing continuous assessment and tracking of data governance maturity. The study advises allocating additional resources and time for further refinement to achieve a fully functional DGMM system. Additionally, the model's implementation and testing should be expanded across diverse MDAs to assess and refine its performance in varied operational contexts.

6.3. Future Research

Future research should address limitations in existing data governance frameworks, particularly in adapting to emerging technologies. Comparative studies across sectors are also recommended to better understand the effectiveness of various data governance practices. Additionally, given the potential for data input bias, research into automating and standardizing user prompts within the DGMM model would help ensure more objective and reliable results. This could enhance the model's utility, mitigating risks associated with user-controlled input biases and contributing to more robust data governance evaluations.

7. Limitations of the Study

The study recognizes several limitations arising from the unique nature of defence operations and the sensitive data involved. Due to strict security protocols, access to data within the Ministry of Defence (MoD) is highly restricted, and obtaining the necessary permissions for data collection requires adherence to stringent approval processes. This need for confidentiality significantly slowed down data gathering and limited the depth and scope of accessible information.

Moreover, certain critical data remained classified, limiting the researcher's ability to comprehensively analyze all aspects of data governance within the MoD. These constraints necessitated a high level of adaptability and caution in research design, as the study ensured that all interactions and data handling strictly complied with military confidentiality standards.

Additionally, the DGMM's focus on the specific challenges of the defence sector may limit its applicability to other industries. The model is tailored to address unique military requirements such as heightened data security, interagency collaboration, and managing data in fragmented, remote environments that are not as prominent in civilian or commercial sectors. Consequently, while the DGMM offers valuable insights into data governance in high-security environments, its utility may be limited outside the defence context.

The model's focus on the MoD's specialized operational environment means that it may not comprehensively address data governance needs in sectors like healthcare or finance, which operate under different regulatory, operational, and data-sharing requirements. Thus, while the DGMM has the potential to set

standards for other sensitive government sectors, its direct generalizability remains constrained to contexts with similar security and operational structures.

Acknowledgements

I am profoundly thankful to God for His constant guidance, which has given me strength and clarity during this educational journey. I extend my sincere gratitude to my supervisors, Prof. Simon Karume from the School of Mathematics & Computer Science at Cooperative University, Dr. Josphat Karani from the School of Pure and Applied Sciences at Kirinyaga University of Kenya for their essential guidance and assistance. I am also grateful to my family for their unwavering support, which has provided immense strength. To my classmates and colleagues, I value the friendship and teamwork that have enhanced my journey. Finally, I express my gratitude to Cooperative University for providing the resources and atmosphere necessary for my research.

Conflicts of Interest

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

References

[1] Alhassan, I., Sammon, D. and Daly, M. (2016) Data Governance Activities: An Analysis of the Literature. *Journal of Decision Systems*, **25**, 64-75. https://doi.org/10.1080/12460125.2016.1187397

[2] Rivera, S., Loarte, N., Raymundo, C. and Dominguez, F. (2017) Data Governance Maturity Model for Micro Financial Organizations in Peru. *Proceedings of the* 19*th International Conference on Enterprise Information Systems*, Porto, 26-29 April 2017, 203-214. https://doi.org/10.5220/0006149202030214

[3] Olaitan, O., Herselman, M. and Wayi, N. (2019) A Data Governance Maturity Evaluation Model for Government Departments of the Eastern Cape Province, South Africa. *SA Journal of Information Management*, **21**, a996. https://doi.org/10.4102/sajim.v21i1.996

[4] MacFeely, S., Me, A., Fu, H., Veerappan, M., Hereward, M., Passarelli, D., *et al.* (2022) Towards an International Data Governance Framework. *Statistical Journal of the IAOS*, **38**, 703-710. https://doi.org/10.3233/sji-220038

[5] Kevins, J. and Brian, K. (2022) Defining Data Protection in Kenya: Challenges, Perspectives and Opportunities. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4270712

[6] Otele, O. (2021) Kenya's Data Protection Regime: Challenges and Future Prospects. *Journal of African Politics*, **1**, 66-88. https://doi.org/10.58548/2021jap101.6688

[7] Tay, C. (2015) Factors Affecting Data Migration in the Kenya Government Ministries. Ph.D. Thesis, University of Nairobi.

[8] Bor, T.K. (2020) Military Involvement in Multi-Agency Security Operations in Eastern Africa: A Case of Kenya Defence Forces. https://erepository.uonbi.ac.ke/handle/11295/154113

[9] Busolo, G. (2019) The Role of Information Security Management System in Promoting African Development: A Case Study of Kenya. Master's Thesis, University of Nairobi.

[10] Duncan, A.D. (2021) Over 100 Data and Analytics Predictions through 2025. https://mpost.io/wp-content/uploads/Gartner-100-data-analytics-predictions-2025.pdf

[11] Abraham, R., Schneider, J. and vom Brocke, J. (2019) Data Governance: A Conceptual Framework, Structured Review, and Research Agenda. *International Journal of Information Management*, **49**, 424-438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

[12] Ekundayo, T., Bhaumik, A., Chinoperekweyi, J. and Khan, Z. (2023) The Impact of Open Data Implementation on Entrepreneurship Ability in Sub-Saharan Africa. *Human Behavior and Emerging Technologies*, **2023**, Article ID: 7583550. https://doi.org/10.1155/2023/7583550

[13] Harland, P.E. and Uddin, Z. (2014) Effects of Product Platform Development: Fostering Lean Product Development and Production. *International Journal of Product Development*, **19**, 259-321. https://doi.org/10.1504/ijpd.2014.064881

[14] Haraguchi, M., Funahashi, T. and Biljecki, F. (2024) Assessing Governance Implications of City Digital Twin Technology: A Maturity Model Approach. *Technological Forecasting and Social Change*, **204**, Article ID: 123409. https://doi.org/10.1016/j.techfore.2024.123409

[15] David Patón-Romero, J., Baldassarre, M.T., Rodríguez, M. and Piattini, M. (2019) Maturity Model Based on CMMI for Governance and Management of Green It. *IET Software*, **13**, 555-563. https://doi.org/10.1049/iet-sen.2018.5351

[16] Moreira, A., Hak, F. and Santos, M.F. (2024) A Maturity Model for Omnichannel Adoption in Health Care Institutions. *Heliyon*, **10**, e38526. https://doi.org/10.1016/j.heliyon.2024.e38526

[17] Sargiotis, D. (2024) Data Governance Maturity Models: Assessing and Enhancing Your Program. In: Sargiotis, D., Ed., *Data Governance*, Springer Nature Switzerland, 487-510. https://doi.org/10.1007/978-3-031-67268-2_17

[18] Al-Ruithe, M. and Benkhelifa, E. (2017) Cloud Data Governance Maturity Model. *Proceedings of the Second International Conference on Internet of Things, Data and Cloud Computing*, Cambridge, 22-23 March 2017, 1-10. https://doi.org/10.1145/3018896.3036394

[19] Permana, R.I. and Suroso, J.S. (2018) Data Governance Maturity Assessment at PT. XYZ. Case Study: Data Management Division. 2018 *International Conference on Information Management and Technology* (*ICIMTech*), Jakarta, 3-5 September 2018, 15-20. https://doi.org/10.1109/icimtech.2018.8528142

[20] Imende-Obonyo, V., Njihia, J.M. and Iraki, X.N. (2024) User Readiness as a Determinant for Use of Big Data Analytics: A Case of State Corporations in Kenya. *The Electronic Journal of Information Systems in Developing Countries*, **90**, 241-267. https://doi.org/10.1002/isd2.12327

[21] Caballero, I., Gualo, F., Rodríguez, M. and Piattini, M. (2023) Maturity Models for Data Governance. In: Caballero, I. and Piattini, M., Eds., *Data Governance*, Springer, 139-162. https://doi.org/10.1007/978-3-031-43773-1_7

[22] Lachaud, E. (2020) ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification. *European Data Protection Law Review*, **6**, 194-210. https://doi.org/10.21552/edpl/2020/2/7

[23] Tachepun, C. and Thammaboosadee, S. (2020) A Data Masking Guideline for Optimizing Insights and Privacy under GDPR Compliance. *Proceedings of the* 11*th International Conference on Advances in Information Technology*, Bangkok, 1-3 July

2020, 1-9. https://doi.org/10.1145/3406601.3406627

[24] Mbanaso, U.M., Abrahams, L. and Okafor, K.C. (2023) Research Philosophy, Design and Methodology. In: Mbanaso, U.M., Abrahams, L. and Okafor, K.C., Eds., *Research Techniques for Computer Science, Information Systems and Cybersecurity*, Springer, 81-113. https://doi.org/10.1007/978-3-031-30031-8_6

[25] Creswell, J.W. (2018) Research Design: Qualitative, Quantitative and Mixed Methods Approaches. SAGE.

[26] Kaushik, V. and Walsh, C.A. (2019) Pragmatism as a Research Paradigm and Its Implications for Social Work Research. *Social Sciences*, **8**, Article 255. https://doi.org/10.3390/socsci8090255

[27] Şahin, M.D. and Ozturk, G. (2022) Mixed Method Research: Theoretical Foundations, Designs and Its Use in Educational Research. *International Journal of Contemporary Educational Research*, **6**, 301-310. https://doi.org/10.33200/ijcer.574002

[28] Mat Roni, S. and Djajadikerta, H.G. (2021) Data Analysis with SPSS for Survey-Based Research. Springer. https://doi.org/10.1007/978-981-16-0193-4

[29] Story, D.A. and Tait, A.R. (2019) Survey Research. *Anesthesiology*, **130**, 192-202.

[30] Clark, A.M. (1998) The Qualitative-Quantitative Debate: Moving from Positivism and Confrontation to Post-Positivism and Reconciliation. *Journal of Advanced Nursing*, **27**, 1242-1249. https://doi.org/10.1046/j.1365-2648.1998.00651.x

[31] Corti, L. and Bishop, L. (2016) Strategies in Teaching Secondary Analysis of Qualitative Data. *Forum Qualitative Sozialforschung*, **6**, Article 47.

[32] De Villiers, M.R. (2012) Models for Interpretive Information Systems Research, Part 2: Design Research, Development Research, Design-Science Research, and Design-based Research—A Meta-Study and Examples. In: Mora, M., Gelman, O., Steenkamp, A.L. and Raisinghani, M., Eds., *Research Methodologies, Innovations and Philosophies in Software Systems Engineering and Information Systems*, IGI Global, 238-255. https://doi.org/10.4018/978-1-4666-0179-6.ch012