

DATA GOVERNANCE FRAMEWORK FOR ECOCAPITAL INVESTMENT MANAGEMENT

JULY 2025

LIMITED

DATA GOVERNANCE GROUP 4

GROUP MEMBERS

Christopher Zanu	11179138
Paula Catherine Bainson	11120453
Stephanie Sakyiwa Ayeh	11257061
Dompreeh Edem	11131220
Salifu Mohammed	11257356
Abdul Samed Al-Hassan Bin Abubakar	11232733
Asare Welbeck	11014502
Zaydan Abass	11099833
Ekua Micah Abakah-Paintsil	11012281
Manga Yobeu Yann Aurel	11004336
Jeremy Elikplim Komla Azumah	11316332

Project Supervisor: DR. Abeeku Sam Edu
OMIS Department
University of Ghana Business School

Laying the Groundwork

UGMC

Our quest began on the 30th of June, 2025. We visited the University of Ghana Medical Centre to submit our introductory letter, given to us by the department. We were able to speak to the receptionist and gave our contact information to them, expecting a response in a week. We did not receive any feedback, so we went scouting for another organization.



KHARIS GLOBAL GROUP

Our next hope was Kharis Global Group, located at Haatso. We visited the organization on the 8th of July and we were able to meet the Business Development Executive, called Mr. Selorm Akorli. He received the letter on behalf of the Operations Manager and promised to give us feedback within the same week. He called two days later to inform us that the Operations Manager was not interested in working with us.



EcoCapital Investment Limited

Moving forward, we visited EcoCapital Investment Limited located at East Legon, on the 14th of July. We had the opportunity to engage the CEO, Compliance Manager, and a Compliance Officer. We had a 3-hour session of detailed Q&A with the aforementioned executives. We were able to gather enough information about their policies, hierarchy, as well as their data protection compliance level. Furthermore, we had access to their existing data governance framework, which served as the basis for building this framework.



1. Executive Summary

EcoCapital Investment Management Limited, a distinguished Ghanaian investment firm, operates at the forefront of investment banking, financial advisory, funds management, and corporate finance. Serving a diverse client base, the company prides itself on core values of integrity, compliance, and client focus. In the highly regulated financial services sector, robust data governance is not merely a regulatory obligation but a strategic imperative that underpins these values, ensuring data integrity, fostering client trust, and maintaining a competitive edge.

An assessment of EcoCapital's current data management landscape reveals commendable strengths, including well-established internal controls, clear segregation of duties, and a resilient data backup infrastructure. The firm's commitment to data availability is evident in its three-server architecture, featuring real-time mirroring between physical and virtual servers for emergency preparedness. However, a recent Data Protection Commission (DPC) Compliance Assessment Report highlighted significant areas for improvement, noting "limited assurance of compliance" with the Data Protection Act 2012 (Act 843), particularly concerning technical and organizational measures. Key deficiencies identified include the absence of a dedicated data management officer and resource constraints related to IT security infrastructure, specifically firewalls.

This report proposes a comprehensive data governance framework for EcoCapital, meticulously aligned with the internationally recognized Data Management Body of Knowledge (DAMA-DMBOK) principles and tailored to Ghana's specific regulatory requirements under the Securities and Exchange Commission (SEC) and the DPC. The framework is structured around critical components: Data Governance Strategy, Data Architecture, Data Security, Data Quality, Data Operations, Data Privacy and Regulatory Compliance, Metadata Management, and Reference and

Master Data Management. The framework's implementation will prioritize establishing a formal Data Governance Council, appointing a dedicated Data Protection Officer (DPO) or Data Management Officer (DMO), and systematically addressing identified technical deficiencies, such as enhancing firewall capabilities. These recommendations aim to elevate EcoCapital's data management maturity, transforming data into a consistently reliable and secure strategic asset.

2. Background and Context

2.1 Introduction to EcoCapital Investment Management Limited

EcoCapital Investment Management Limited stands as a premier investment firm in Ghana. With a team of 21 employees, the company is deeply engaged in investment banking, investment management, financial advisory, funds management, and corporate finance. Its service offerings extend to investment research, advisory, and business acquisition for a diverse clientele. The firm's operational philosophy is firmly rooted in its core values: integrity, compliance, and client focus.

These values are not merely aspirational but are foundational to every aspect of the company's operations.

Operating within the Capital Market and Pension fund management sectors, EcoCapital is inherently exposed to stakeholders who possess a profound interest in the meticulous management of information, especially client data. Clients, in particular, hold an expectation that the information they entrust to EcoCapital will be handled with the "highest level of confidentiality and professionalism". This expectation underscores the critical importance of a robust data governance framework that not only meets regulatory demands but also reinforces the trust placed in the firm by its clients.

2.2 The Ghanaian Regulatory Landscape

EcoCapital operates within a dual regulatory environment, subject to the oversight of both the Securities and Exchange Commission (SEC) and the Data Protection Commission (DPC) in Ghana. Navigating the requirements of these two distinct bodies necessitates a comprehensive and integrated approach to data management.

Securities and Exchange Commission (SEC)

The SEC serves as the primary regulator for investment companies and investment advisers in Ghana. Its mandate is expansive, encompassing the assurance of transparency in financial and operational risk, and requiring regulated entities to provide detailed data and granular analysis of their operations. The Commission also prescribes specific record-keeping requirements to ensure accountability and oversight.

Data Protection Commission (DPC)

The DPC is an independent statutory body established under the Data Protection Act (DPA) 2012 (Act 843). Its core function is to safeguard individual privacy and personal data by regulating how such information is processed. EcoCapital is duly registered with the DPC under ID DC16080000551E, affirming its legal obligation to comply with the Act.

Inter-Regulatory Protocol for Data Disclosure

A unique and critical aspect of EcoCapital's regulatory compliance is the explicit requirement for inter-regulatory data disclosure. As stipulated by the company's operational guidelines, "Whenever the SEC request for client info as their regulator, the company still have to write to the DPC informing them of the development before handing over the data. This requirement extends beyond the general provision in Section 21(2)(a) of the DPA, which permits data disclosure when "required by law".

2.3 The Importance of Data Governance in Investment Banking

In investment banking, data is a strategic asset that drives decision-making, client insights, and competitive advantage. Effective data governance is essential for managing risks such as breaches, regulatory non-compliance, inefficiencies, and reputational harm.

3. Governance Challenge and Stakeholder Analysis

3.1 Current State of Data Management at EcoCapital

EcoCapital has established several commendable practices and controls within its existing data management landscape, yet a recent regulatory assessment has also highlighted critical areas requiring immediate attention and improvement.

Strengths and Existing Controls

EcoCapital demonstrates a foundational commitment to a robust control environment, characterized by a strong governance culture and a robust process throughout its business operations. Key strengths include:

- ✓ **Segregation of Duties:** The firm explicitly implements "segregation of duties across business units" with "clearly defined duties and responsibilities of all staff". This is reinforced by the policy that "no single person is permitted to handle all aspect of a transaction or sensitive data changes". This structure minimizes the risk of internal fraud and error.
- ✓ **Access Control:** Existing practices ensure that only authorized individuals have physical access to computer networks, equipment, and storage devices. Employee access rights are restricted to their specific functions, requiring supervisor approval for system access, and user profiles are periodically reviewed. Each employee is assigned a unique alphanumeric ID and password, and different levels of access are enforced across the organization.
- ✓ **Data Verification:** A critical data quality control is the verification of information prior to entry, exemplified by the use of Ghana Card ID for client onboarding processes.
- ✓ **Backup and Recovery:** EcoCapital maintains a resilient infrastructure with three servers—physical, virtual, and backup. The physical server mirrors the virtual server in real-time "just in case of an emergency," providing immediate failover capability. Furthermore, data and system backups are performed and tested regularly, with offsite storage utilized for disaster recovery purposes.
- ✓ **Audit Trails:** The system is configured to leave a trail of evidence whenever an employee makes changes to the database. System logs are periodically printed and reviewed by management as part of monitoring and evaluation.
- ✓ **Confidentiality Principle:** The inherent nature of the investment industry dictates a high level of confidentiality in the handling of all kinds of information, ensuring that data is well safeguarded.

Identified Gaps and Areas for Improvement

Despite these commendable existing controls, the Data Protection Commission's Compliance

Assessment Report identified several crucial areas where EcoCapital's data protection posture requires significant enhancement:

- ✓ **Limited DPA Compliance:** While some controls exist, they lack formal documentation, strategic integration, and comprehensive application, leading to only *"limited assurance of compliance"* with the Data Protection Act (Act 843). This weakens EcoCapital's regulatory standing.
- ✓ **No Designated Data Management Officer:** The absence of a permanent, certified officer creates a leadership vacuum in data governance. Without a dedicated figure, compliance efforts are fragmented, and accountability is unclear.
- ✓ **Inadequate IT Security Resources:** There are significant shortfalls in essential infrastructure—most notably, the lack of modern firewalls. This exposes EcoCapital to cyber threats and unauthorized data access. High implementation costs have delayed upgrades.
- ✓ **Lack of Comprehensive Policies:** Organizational policies around data protection are underdeveloped or inconsistently applied. Without clearly defined, documented, and enforced policies, data governance cannot be effectively operationalized across departments.
- ✓ **Missing DPIA and PIMS Structures:** The DPC recommends that EcoCapital implement both a Data Protection Impact Assessment (DPIA) framework and a Personal Information Management System (PIMS). These tools are essential for proactively identifying privacy risks and tracking compliance.
- ✓ **Unformalized Data Lifecycle Management:** Although EcoCapital retains and disposes of client data in line with Ghanaian laws, these practices are not fully embedded into a formal, auditable lifecycle framework—affecting consistency and legal defensibility.

3.2 Organizational Structure and Data Roles

Table 1: EcoCapital Organizational Structure with Data Governance Responsibilities

Organizational Role	Existing Reporting Line (from chart)	Key Data Responsibilities	Current Data Access Level	Proposed Data Governance Role
Board	Top-level	Ultimate responsibility	N/A (Strategic Oversight)	Executive Oversight

		for internal controls & data strategy commitment		
CEO	Reports to Board	Ultimate accountability for data assets; strategic direction; payment authorization.	Read/Write (Most Data)	Data Owner, Executive Sponson
COO	Reports to CEO	Oversees operational data processes; resource allocation for data initiatives	Read/Write (Operational Data)	Executive Sponsor, Operational Lead
Compliance Manager	Reports to CEO	Oversees regulatory risk & control; approves data-related changes; DPC/SEC liaison; client data protection.	Read/Write (Most Data)	Lead Data Steward, DPO Designate
IT Department	Reports to CEO	Manages data infrastructure; ensures data availability, security (firewalls); access control	Read (Database), Write (System Config)	Data Custodian

		implementation		
H.R.	Reports to COO	Manages employee data lifecycle (hard copies locked)	Hard Copy Only (Employee Data)	Data Steward (Employee Data)
Fund Manager	Reports to COO	Manages trade accounts; ensures transaction authorization & processing; uses client/account info for trades	Write (Trade Accounts Only)	Data Steward (Trade Data)
Marketing	Reports to COO	Utilizes client data for marketing; ensures consent for communications	Read/Write (Marketing Data)	Data User, Data Steward (Marketing Data)
Client Service	Reports to Marketing	First point of contact for clients; manages client relationships; provides info to Fund Manager	Read/Write (Client Interaction Data)	Data Steward (Client Interaction)
Accounts	Reports to Marketing	Manages customer financial	Read/Write (Customer	Data Steward (Financial

		accounts; ensures accurate recording & reconciliation; calculates fees	Accounts)	Data)
Portfolio Manager	Reports to Fund Manager	Manages client portfolios; handles sensitive investment data	Read/Write (Portfolio Data)	Data Steward (Portfolio Data)
Research	Reports to Portfolio Manager	Conducts investment research; responsible for client data protection in research context	Read/Write (Research Data)	Data Steward (Research Data)
Portfolio Analyst	Reports to Portfolio Manager	Supports portfolio management and analysis	Read (Portfolio Data)	Data User
Admin	Reports to Accounts	General administrative support; handles various data types	Read/Write (Admin Data)	Data User
Front Desk	Reports to Accounts	Initial client interaction; handles basic	Read (Basic Client Data)	Data User

		client information		
--	--	-----------------------	--	--

External Stakeholders

- ✓ **Clients:** Clients expect that their personal and transactional data are kept confidential and properly protected, all the while protecting their rights specified in Data Protection Act (Act 843).
- ✓ **Securities and Exchange Commission (SEC):** SEC as a primary regulator is particularly interested in how EcoCapital adheres to all securities laws, financial transparency, risk mitigation strategies, and robust record-keeping practices.
- ✓ **Data Protection Commission (DPC):** DPC is interested in ensuring that EcoCapital fully complies with the Data Protection Act 2012 (Act 843), particularly with regards to data privacy safeguards, lawful processing of personal data, and the implementation of appropriate technical and organizational measures.
- ✓ **National Pensions Regulatory Authority (NPRA):** NPRA as a key regulator is specifically interested in how EcoCapital properly manages pensions funds and how data related to pension schemes and beneficiaries are protected.
- ✓ **External Auditors (e.g., Transcend Chartered Accountants):** These entities are interested in the accuracy and integrity of financial data, the effectiveness of internal controls, and overall compliance with accounting standards and regulatory requirements.
- ✓ **Service Providers (e.g., Norbus Consult Ltd for NAM):** Interested in data integration, system functionality, and the security of data exchanged or managed through their platforms.

4. Proposed Data Governance Framework

4.1 Introduction to DAMA-DMBOK Principles

The proposed Data Governance Framework for EcoCapital Investment Management Limited is based on the **DAMA-DMBOK (2nd Edition)**, a globally recognized and vendor-neutral guide to data management best practices. Within DAMA-DMBOK, Data Governance is the central coordinating function, ensuring consistency across all data-related activities. This foundation provides standardized terminology and role clarity, which are essential for promoting consistent data practices across EcoCapital.

However, while DAMA-DMBOK is comprehensive, it is not a prescriptive standard and offers limited tactical execution guidance. Therefore, EcoCapital will adapt the framework to suit its size (21 employees) and specific operational and regulatory context. A phased, practical implementation will be used to manage complexity, achieve early wins, and foster organizational buy-in.

4.2 Core Components of the EcoCapital Data Governance Framework

4.2.1 Data Governance Strategy & Organization

1. Data Governance Council

A **Data Governance Council** will be established to provide strategic direction, approve policies, resolve issues, and monitor compliance. This directly responds to the DPC's recommendation to embed data governance as a core part of the organization.

- ✓ **Composition:** CEO (as Data Owner), Compliance Manager (as DPO designate), COO, Head of IT, and a senior finance or fund management representative.
- ✓ **Meetings:** Quarterly, to review data quality, security incidents, and compliance status.

2. Defined Data Roles

Formal data roles ensure accountability and smooth execution across the organization:

- ✓ **Data Owner (CEO):** Ultimate accountability for data quality, security, and compliance.
- ✓ **Data Protection Officer (DPO):** A permanent role managing Data Protection Act compliance and liaising with the DPC.
- ✓ **Data Stewards:** Department heads (e.g., Compliance, HR, Operations) responsible for day-to-day data governance in their domains.
- ✓ **Data Custodians (IT):** Oversee technical implementation, availability, and security of data systems.
- ✓ **Data Users (All Staff):** Must comply with all data-related policies and procedures.

3. Data Governance Policies and Procedures

To address existing policy gaps, several key policies will be developed:

- ✓ **Data Classification:** Categorizing data based on sensitivity and criticality.
- ✓ **Access Management:** Clear roles, permissions, and regular access reviews.
- ✓ **Data Retention & Disposal:** Formalize the 7-year retention rule and secure disposal methods.
- ✓ **Data Quality Management:** Procedures for validation, correction, and ongoing monitoring.
- ✓ **Incident Response:** Defined steps for breach detection, response, and reporting.
- ✓ **Privacy & Consent:** Managing data subject consent in line with Data Protection Act 2012.
- ✓ **Change Management:** Formal approval processes for system or policy changes, led by the Compliance Manager.

4.2.2 Data Architecture

Data architecture provides the foundational structure for integrating data systems, ensuring scalability, integrity, and consistency. A core principle of this component is "Security, Privacy, and Compliance by Design", integrating data protection measures from the outset.

- ✓ **Data Platforms and Storage Strategies:**
 - **Norbus Asset Management Suite (NAM):** Data architecture principles must explicitly apply to all data residing within NAM, which is recognized as EcoCapital's primary investment accounting system, including its security configurations, access controls, and data quality standards.
 - **Server Infrastructure:** The current server setup, a critical component of the firm's data architecture comprises of the physical, virtual, which mirrors the physical in real-time, and backup servers provides a robust mechanism for business continuity and disaster recovery in emergency scenarios.
 - **Offsite Storage:** The existing practice of storing all gathered data at an offsite location for recovery purposes in case of an emergency will be formalized within the data architecture. This ensures data availability and resilience against unforeseen events.
- ✓ **Data Flow Diagrams and Integration Patterns:** EcoCapital will map critical data flows to ensure seamless data management, documenting key processes like client onboarding and regulatory reporting. This includes analyzing data exchange between departments and external entities, such as SEC, DPC, NPRA, brokers and custodians.
- ✓ **Architectural Principles:** The data architecture will be designed with inherent support for data quality, security, and regulatory compliance, aligning with industry best practices (DAMA-DMBOK).

EcoCapital's existing server infrastructure, with real-time mirroring, regular backups, and offsite storage provides a robust foundation for data resilience, availability, and disaster recovery, supporting business continuity and strengthening data governance.

DATA SECURITY

Data security is paramount in the investment sector, aiming to enable appropriate access while preventing unauthorized access, ensuring data privacy and confidentiality, and adhering to relevant regulations.

- **Security Policies and Procedures:**
 - ✓ **Access Control:** Detailed procedures for granting, modifying, and revoking access will be documented and strictly enforced. For example, Fund Managers will continue to be restricted to making changes only to trade accounts, IT personnel will maintain read-only access to the database, Accounts will retain read and write access to customer accounts, and HR will manage hard copies of employee data in a locked room.
 - ✓ **Network Security:** Addressing the identified deficiency in firewalls, the framework will prioritize the implementation of robust firewalls and other intrusion detection/prevention software to safeguard the local network from unauthorized access and malicious electronic attacks.
 - ✓ **Data Encryption and Masking:** Explore and implement techniques such as encryption and data masking for sensitive data to reduce exposure and enhance protection.

- ✓ **Security Monitoring and Auditing:** Regular monitoring of user authentication and access behavior, coupled with periodic review of system logs, will be formalized to detect and respond to suspicious activities. Security policies will be auditable and regularly audited to ensure compliance.
- ✓ **Incident Management:** Develop a comprehensive incident response plan to promptly address and rectify any data breaches or security incidents, including clear protocols for internal reporting and external notification to regulators (e.g., DPC) and affected data subjects.
- **Data Classification for Security:** Implement a formal data classification scheme based on sensitivity levels (e.g., public, internal, confidential, restricted).
- **Employee Training and Awareness:** Regular and mandatory training programs will be conducted to educate all employees on data security policies, best practices, and their individual responsibilities in protecting sensitive information.

4.2.3 DATA QUALITY

Data quality ensures that data is accurate, complete, consistent, timely, and relevant for its intended use, which is critical for reliable decision-making and regulatory compliance in investment banking.

- **Data Quality Dimensions:** Define and measure data quality across key dimensions:
 - ✓ **Accuracy:** Ensuring data correctly reflects the real-world facts (e.g., verified Ghana Card ID for client onboarding).
 - ✓ **Completeness:** Ensuring all required data elements are present.
 - ✓ **Consistency:** Ensuring data values are uniform across different systems and contexts.
 - ✓ **Timeliness:** Ensuring data is available when needed and up-to-date.
 - ✓ **Validity:** Ensuring data conforms to defined formats, types, and ranges.
- **Data Quality Processes:**
 - ✓ **Data Verification at Entry:** Formalize and strengthen existing practices for verifying information at the point of entry, such as the use of Ghana Card ID for client identification.
 - ✓ **Regular Data Audits and Profiling:** Conduct periodic audits and profiling of key data sets (e.g., client information, transactional data) to identify quality issues.
 - ✓ **Error Detection and Correction:** Establish clear procedures for detecting data errors, assigning responsibility for correction (e.g., Data Stewards), and tracking resolution.
 - ✓ **Data Reconciliation:** Formalize and enhance existing reconciliation processes, such as the 3-way reconciliation between EcoCapital, the Trustee, and the Custodian for cash and security positions. Investment income reconciliation and stale price testing are also critical existing controls to be formalized.
- **Data Quality Roles:** Data Stewards (e.g., Fund Manager, Accounts, Client Service) will be explicitly responsible for data quality within their domains, reporting issues to the Data Governance Council.

4.2.4 DATA OPERATIONS

Data operations encompass the planning, deployment, and management of structured physical data assets and their underlying infrastructure, ensuring efficient and reliable data processing.

- **Data Storage and Management:**
 - ✓ **Server Management:** Continue and enhance the management of physical, virtual, and backup servers, ensuring real-time mirroring and regular testing for recoverability.
 - ✓ **Offsite Data Storage:** Formalize the procedures for offsite storage of all gathered data for disaster recovery purposes, including regular verification of offsite backups.
 - ✓ **System Monitoring:** Implement enhanced monitoring of IT hardware and software issues to ensure timely resolution and minimize operational interruptions.
- **Data Processing and Workflow:**
 - ✓ **Transaction Processing:** Formalize and continuously optimize the processes for securities and cash transaction processing, ensuring proper authorization, accurate recording, and timely settlement.
 - ✓ **Corporate Actions:** Ensure timely and accurate processing of corporate actions received from external sources, with regular reconciliation against custodian and broker records.
- **System Access Management:** Continuously review and update employee access rights based on changes in job roles and workflows.

4.2.5 Data Privacy & Regulatory Compliance

This component ensures EcoCapital's adherence to the Data Protection Act 2012 (Act 843) and SEC regulations, safeguarding personal data and respecting data subject rights.

- **DPC Registration and Renewal:** Ensure timely renewal of DPC registration every two years.
- **Data Protection Principles Adherence:** Integrate and enforce the eight data protection principles of Act 843: Accountability, Lawfulness of Processing, Specification of Purpose, Compatibility of Further Processing, Quality of Information, Openness, Data Security Safeguards, and Data Subject Participation.
- **Consent Management:** Establish clear processes for obtaining, documenting, and managing data subject consent for personal data processing, ensuring that processing is only done with prior consent unless legally mandated otherwise.
- **Data Subject Rights:** Develop procedures to facilitate data subjects' exercise of their rights, including the right to be informed, access personal data, amend data, object to processing, prevent processing for direct marketing, and complain.
- **Regulatory Reporting and Disclosure:**
 - ✓ **SEC Reporting:** Ensure all SEC-mandated reports and disclosures, including client KYC details, client mandates, and investment management agreements, are accurate and timely.
 - ✓ **Inter-Regulatory Data Sharing Protocol:** Formalize the specific protocol for data disclosure to regulators: "Whenever the SEC request for client info as their regulator, the

company still have to write to the DPC informing them of the development before handing over the data".

- ✓ **Change in Management Notification:** Formalize the process for notifying the SEC in writing of any change in management.
- **Data Retention and Disposal:** Reinforce the policy of retaining former client data for 7 years as per Ghanaian Data Protection laws, and ensure hard copies are shredded under surveillance while soft copies are wiped from the system with code.
- **PIMS Implementation:** Implement a Personal Information Management System (PIMS) to effectively manage and demonstrate compliance with DPA requirements, including staff training and awareness on data protection.

4.2.6 METADATA MANAGEMENT

Metadata, or "data about data," is crucial for understanding, managing, and leveraging data assets. It provides context, meaning, and lineage for all data within the organization.

- ✓ **Metadata Collection and Categorization:** Establish processes for collecting, categorizing, and maintaining metadata across all data assets, including business, technical, and operational metadata.
- ✓ **Business Glossary:** Develop and maintain a comprehensive business glossary to standardize terminology and definitions across the organization, ensuring a shared understanding of key data elements. This supports DAMA-DMBOK's emphasis on "standardized terminology".
- ✓ **Data Lineage:** Document data lineage to track the origin, transformations, and movement of data through its lifecycle, which is essential for auditing, troubleshooting, and ensuring data quality.

4.2.7 Reference & Master Data Management

Managing shared data consistently is vital for reducing redundancy and ensuring data quality across the organization.

- ✓ **Reference Data Management:** Establish processes for managing reference data (e.g., country codes, currency codes, industry classifications) to ensure consistency and accuracy across all systems and reports.
- ✓ **Master Data Management:** Implement strategies for managing master data (e.g., client master data, product master data) to create a single, authoritative view of critical business entities. This reduces redundancy and enhances data quality through standardized definitions and use of data values.
- ✓ **Data Standardization:** Promote the use of standardized data values and formats, especially for client profiling information such as Ghana Card ID.

5. Implementation Roadmap

This roadmap outlines the key steps to transition from the current state to a more effective data governance environment.

5.1 Phase 1: Assessment and Planning (Months 1-3)

- ✓ **Data Management Maturity Assessment:** Conduct a thorough assessment of EcoCapital's current data management practices across all DAMA-DMBOK knowledge areas, building upon the DPC's findings. This will identify specific gaps and areas requiring improvement beyond those already noted in the DPC report.
- ✓ **Executive Sponsorship and Data Governance Council Formation:** Secure explicit executive sponsorship from the Board and CEO. Formally establish the Data Governance Council, defining its charter, scope, and initial priorities.
- ✓ **DPO/DMO Appointment and Empowerment:** Formally appoint a dedicated Data Protection Officer (DPO) or Data Management Officer (DMO), transitioning from the interim role. Provide this individual with the necessary authority, resources, and training to fulfill their responsibilities.

5.2 Phase 2: Foundation Building and Policy Development (Months 4-9)

- ✓ **Policy Development and Documentation:** Develop and formally document comprehensive data governance policies and procedures identified in Phase 1. This includes detailed policies for data access, retention, disposal, data quality, and incident response.
- ✓ **Role Definition and Training:** Clearly define and communicate the responsibilities of all data roles (Data Owners, Data Stewards, Data Custodians, Data Users) as outlined in Table 1. Initiate targeted training programs for all employees on data protection principles, new policies, and their specific data responsibilities.

5.3 Phase 3: Implementation and Operationalization (Months 10-18)

- ✓ **Data Quality Program Rollout:** Implement data quality processes, including automated data validation rules within systems (e.g., NAM), regular data profiling, and a structured approach to error detection and correction.
- ✓ **Inter-Regulatory Protocol Operationalization:** Conduct internal workshops and drills to ensure all relevant personnel understand and can execute the specific protocol for notifying the DPC before disclosing client information to the SEC.
- ✓ **Continuous Monitoring and Reporting:** Establish key performance indicators (KPIs) for data governance, data quality, and security. Implement regular reporting mechanisms to the Data Governance Council and executive leadership on compliance status and performance.

5.4 Phase 4: Optimization and Continuous Improvement (Ongoing)

- ✓ **Regular Policy Review and Updates:** Data governance policies and procedures will be regularly reviewed and updated to reflect changes in regulatory requirements, technological advancements, and business operations.
- ✓ **Advanced Data Quality Initiatives:** Explore and implement advanced data quality initiatives, such as predictive analytics for data anomalies and automated data cleansing routines.

- ✓ **Security Posture Enhancement:** Continuously assess and enhance the firm's security posture through regular vulnerability assessments, penetration testing, and staying abreast of emerging cyber threats.
- ✓ **Employee Awareness Reinforcement:** Conduct ongoing training and awareness campaigns to maintain a high level of data literacy and security consciousness among all employees.

6. Risks and Ethical Considerations

Implementing a comprehensive data governance framework, while essential, is not without its challenges and ethical considerations. Proactive identification and mitigation of these factors are crucial for successful adoption and sustained compliance.

6.1 Key Risks

- ✓ **Resource Constraints:** EcoCapital's status as a small firm with 21 employees implies potential limitations in dedicated resources (financial, human, and technological) for a full-scale data governance implementation. The "high cost of putting in place IT systems like firewalls" has already been identified as a barrier. Without adequate investment, the framework's effectiveness may be compromised.
- ✓ **Organizational Resistance to Change:** Implementing new policies, procedures, and roles can encounter resistance from employees accustomed to existing workflows. A "longer onboarding curve" is a known challenge with DAMA-DMBOK adoption, requiring significant change management. Lack of understanding or perceived increased workload could hinder adoption.
- ✓ **Technological Obsolescence and Evolution:** The rapid pace of technological change means that implemented solutions may quickly become outdated. The framework must be agile enough to adapt to new technologies and emerging data management practices, especially given the "less emphasis on automation" in DAMA-DMBOK's traditional approach.
- ✓ **Data Breach Risk:** Despite enhanced security measures, the risk of data breaches remains. Human error, sophisticated cyber-attacks, or insider threats can compromise data integrity and confidentiality, leading to severe financial, reputational, and legal consequences.

6.2 Ethical Considerations

- ✓ **Client Privacy and Trust:** As a "top-notch investment firm" with "client focus" as a core value, EcoCapital has a profound ethical obligation to protect client data. Mismanagement of data could severely damage this trust and the firm's reputation.
- ✓ **Transparency with Data Subjects:** The DPA 2012 (Act 843) emphasizes "Openness" and "Data Subject Participation." Ethically, EcoCapital must be transparent with clients about how their data is collected, processed, stored, and used.
- ✓ **Fair Data Processing:** Ethical data processing requires that data is collected for "specific, explicitly defined and lawful" purposes, and that further processing is "compatible with the purpose of collection". This prevents misuse of data beyond the scope for which it was

originally provided.

- ✓ **Accountability and Responsibility:** Clearly defining data roles and responsibilities is not just for operational efficiency but also for ethical accountability. When data issues arise, it must be clear who is responsible for addressing them, fostering a culture of ownership and integrity.
- ✓ **Balancing Regulatory Demands and Privacy:** The requirement to notify the DPC before handing over data to the SEC presents an ethical balancing act. While regulatory compliance is paramount, the firm must ensure that this process is handled with the utmost care for client privacy, even when legally compelled to disclose. The SEC itself notes it "must balance the rights of its data subjects against other competing rights because of the public interest nature of its mandate." EcoCapital must navigate this balance ethically.

7. Conclusion and Recommendations

EcoCapital Investment Management Limited operates in a highly regulated environment where data is both a strategic asset and a significant liability if not managed effectively. While the firm possesses commendable foundational controls, a recent DPC assessment highlighted critical areas requiring immediate attention, particularly concerning comprehensive DPA compliance and IT security infrastructure. The proposed data governance framework, built upon DAMA-DMBOK principles and tailored to Ghana's SEC and DPC regulations, offers a structured pathway to enhance EcoCapital's data management maturity. It emphasizes establishing a formal Data Governance Council, clearly defining data roles, and developing comprehensive policies covering the entire data lifecycle. By addressing the identified gaps, EcoCapital can elevate its compliance posture, and reinforce its reputation for integrity and client focus.

Based on the analysis, the following recommendations are put forth to guide EcoCapital's implementation of the proposed data governance framework:

I. Formalize Data Governance Structure:

- ✓ **Recommendation:** Immediately establish a formal Data Governance Council, comprising the CEO, Compliance Manager, COO, Head of IT, and a senior representative from Fund Management/Accounts.
- ✓ **Action:** Define the Council's charter, meeting cadence (e.g., quarterly), and authority to approve data governance policies and resolve data-related issues.
- ✓ **Impact:** Provides top-down commitment and strategic direction, addressing the DPC's call for data protection as a core governance feature.

II. Appoint and Empower a Dedicated DPO/DMO:

- ✓ **Recommendation:** Transition the "interim officer" role into a permanent, dedicated Data Protection Officer (DPO) or Data Management Officer (DMO) position.
- ✓ **Action:** Provide the DPO with adequate resources, formal authority, and specialized training to oversee DPA compliance, manage data protection policies, and act as the

primary liaison with the DPC.

- ✓ **Impact:** Directly addresses the critical "absence of a designated data management officer", ensuring continuous and expert oversight of data protection.

III. Enhance IT Security Infrastructure:

- ✓ **Recommendation:** Prioritize investment in and implementation of robust firewalls and other necessary intrusion detection/prevention systems.
- ✓ **Action:** Develop a phased implementation plan and allocate sufficient budget to address the main resource deficiencies in firewalls.
- ✓ **Impact:** Strengthens technical and organizational measures, directly improving the "limited assurance of compliance" noted by the DPC and protecting against unauthorized access.

IV. Develop Comprehensive Data Policies and Procedures:

- ✓ **Recommendation:** Create and formally document a complete suite of data governance policies and procedures.
- ✓ **Action:** Focus on policies for data classification, detailed access management (building on existing unique IDs and varied access, data retention and disposal (formalizing the 7-year rule and secure destruction methods), data quality management, and a robust incident response plan.
- ✓ **Impact:** Addresses the "lack of adequate organizational policies and programs", providing clear guidelines for all data-related activities.

V. Sustain Continuous Improvement and Training:

- ✓ **Recommendation:** Embed a culture of continuous improvement for data governance.
- ✓ **Action:** Conduct regular data governance maturity assessments, provide ongoing employee training and awareness programs on data protection and security, and regularly review and update policies to adapt to evolving regulatory landscapes and technological advancements.
- ✓ **Impact:** Ensures long-term sustainability of the data governance program, maintaining high data quality, security, and compliance in a dynamic environment.

By implementing these recommendations, EcoCapital Investment Management Limited can strengthen its operational resilience, enhance client trust, and solidify its position as a leading, integrity-driven investment firm.

REFERENCES

Data Protection Commission. (2012). *Data Protection Act, 2012 (Act 843)*.
<https://dataprotection.org.gh/data-protection/>.

Data Protection Commission. (n.d.). *Home*. <https://dataprotection.org.gh/>

Data Protection Compliance Report.pdf

DAMA International. (2017). *DAMA-DMBOK: Data management body of knowledge* (2nd ed.). Technics Publications. <https://dama.org/learning-resources/dama-data-management-body-of-knowledge-dmbok/>

DAMA Denmark. (n.d.). *DAMA-DMBOK2 PDF*. [https://www.dama-dk.org/onewebmedia/DAMA%20DMBOK2_PDF.pdf](https://www.dama.dk.org/onewebmedia/DAMA%20DMBOK2_PDF.pdf)

EcoCapital Internal Control (Under Review).pdf

Securities and Exchange Commission Ghana. (2008). *SEC compliance manual for broker-dealers, investment advisers & representatives* (January 2008). https://sec.gov.gh/wp-content/uploads/Final-Regulatory-Laws/Codes/SEC_Compliance%20Manual_January_2008.pdf

Securities and Exchange Commission Ghana. (2021). *Investment guidelines for fund managers* (SEC/GUI/001/07/2021). https://sec.gov.gh/wp-content/uploads/Final-Regulatory-Laws/Guidelines/INVESTMENT_GUIDELINES_FOR_FUND_MANAGERS.pdf