Data Risk Governance Framework

Approved By	Group Chief Risk Officer
Document Owner	Group Chief Risk Officer
Document Author	Group Risk
Effective Date	1 May 2024

Version Control

Version no.	Date issued	Key Revisions
1.0	27 April 2022	First issuance (Regina Phua)
2.0	23 May 2023	Annual refresh (Sarah Cheong) Aligned document format to Policy Document Template 1.3d) added reference to third party data breach 1.3e) added "procedures" 2.2 First LOD – renamed Technology Office role-holder 2.2 Second LOD – DPO role revised and reference Privacy Policy, amended IT risk feedback role, Compliance to Privacy compliance 2.3 – Framework and policies combined with Section 6 to form Section 6 – Framework, Policy and related documents. 6.0 Updated document name and owners. 7.0 – Version control moved to page 2 and Section 7 replaced with 7.0 – Review 8.0 – Added section for Non-compliance
3.0	1 May 2024	Updates (Daniel Heng) - Editorial changes across the Framework to improve clarity - 2.1 Governance Structure - Updated - 2.2 Roles and Responsibilities – • Updated Data Owner on Marketing Campaign/Servicing Campaign approval, and Data Quality Procedures • Data Steward – Newly added • Renamed Data Risk Team and IT Risk Team to Group Risk and Tech Risk respectively - 3.2 Data Lifecycle Management – Updated Data Inventory Documents

Contents

1. Purpose, Scope and Principles

1.1 Purpose

Singapore Life Holdings Pte. Ltd. And its group of companies (collectively labelled as the "Group") seeks to optimise its performance while remaining within risk appetite and meeting the expectations of stakeholders. This is achieved by embedding rigorous and consistent risk management practices (including risk culture and risk strategy) in accordance with the Group Risk Management Framework.

This Data Risk Governance Framework ("Framework") is supported by three core pillars (i) data management; (ii) data privacy; and (iii) information security which collectively supports the Group in managing data risks. The focus of this Framework is primarily on Critical Data and Personal Data.

It is the management's responsibility to ensure this Framework is implemented in their respective companies and sufficient documented evidence is maintained to demonstrate effective data risk governance and management.

1.2 Scope

The scope of this Framework is Group-wide. It applies to all companies within the Group, their operations, functions and employees.

It is recognised that in some countries, local legislation, regulations and governance practices may prohibit the direct adoption of this Framework in its entirety. In such cases, the board and senior management of the legal entity shall adopt this Framework to the extent permitted by local law and regulations. In any event, the board and senior management of the legal entity has an obligation to define the risk governance framework for the entity, and it is expected that such a framework should satisfy the principles and requirements set out in this Framework. The opinion of the Group Chief Risk Officer ("CRO") as the representative of the ultimate parent company/shareholder must be sought through the modifications and exceptions process, where such a local framework deviates from the terms of this Framework.

1.3 Principles

To facilitate the achievement of risk management goals in accordance with the Group Risk Management Framework, the following principles must be observed at all times:

a. While data brings business opportunities, it also introduces material risks to the group/ company. All data users must ensure that the potential risks are well understood and effective controls implemented to address the underlying risk drivers;

b. All data must be classified as either Critical or Non-Critical data. Critical Data, including Personal Data, must be properly safeguarded and used only for authorised purposes;

c. Personal Data factored into business modelling and decision-making must be used responsibly, ethically and complies with all applicable regulatory expectations;

d. All data breach events and data incidents, including data breach events by our third party suppliers, must be reported on a timely basis and handled in accordance with the local regulatory obligations. The root-cause of the event must be properly identified and appropriate controls implemented to prevent repeated occurrences;

e. Policies, standards, guidelines and procedures must be developed to drive consistency in data risk governance and management practices across the Group and in line with local regulatory obligations.

This Framework seeks to support the Group in meeting its business objectives and sustainability agenda through data that is appropriately managed and protected.

2. Data Risk Governance

Data risk governance is about defining the policies, structure and processes for ensuring ownership, accountability, controls and oversight of data through its lifecycle. Embedding data risk governance across the companies in the Group provides a consistent basis on which the Group can understand what data it has, who owns it, how it is stored, whether it is of good quality, what purpose it is used for and whether it is retained and destroyed in line with regulatory requirements.

2.1 Governance Structure (Updated)

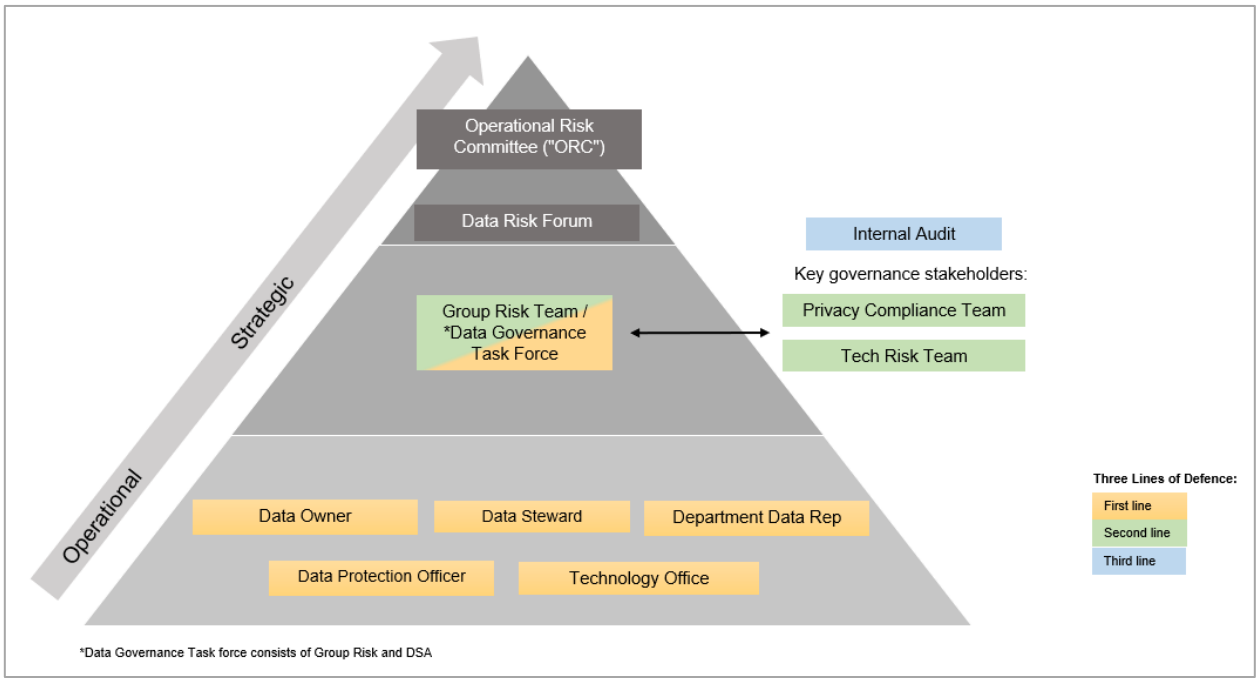

Figure 1: Overview of Group Data Risk Governance Structure

2.2 Roles and Responsibilities

Committee and Forum

Committee/Forum	Responsibilities
Operational Risk Committee ("ORC")	• Oversees the Group's data risk profile. Direct actions as necessary to mitigate risk exposure to the desired level. • Provides strategic direction and guidance for the management of data risk across the Group.
Data Risk Forum	• A platform for the Key Data Governance Stakeholders, Data Owners, Data Protection Officers and Department's Data Representatives to convene, share and discuss matters related to data risk governance and management. Collectively, the Data Risk Forum is responsible for driving effective controls over the management of Critical Data and Personal Data owned or controlled by the Group. • Escalates issues for advice or decision, and if required, to CRO and/or ORC for endorsement/decision. Each OpCo member is responsible for appointing suitable [1]Data Owners and Data Protection Officers for their respective functions. [1]Appointed Data Owner should be of sufficient seniority to carry out the responsibilities

First Line of Defence

Role	Responsibilities
Technology Office	• Designs and regularly reviews the information security policy and data security standard. • Implements appropriate technical safeguards to protect the confidentiality, integrity and availability of information asset and data. • Manages data user access as prescribed and authorised by data owners (applies to systems managed by IT). • Overall responsible for monitoring and managing data security to ensure that the IT operating environment is secured. • Provides technical support for data management.
Data Owner	• Exercises full oversight, accountability, and [1]approval authority for the data assets they own.

Role	Responsibilities
	• Ensures that the data assets they own is governed effectively across all systems and lines of business. • Responsible for mitigating risk exposure, improving efficiency, maintaining data integrity and maximising [2]data quality to ensure data assets continually add value to business operations and the consumers of the data. • Responsible for the oversight and application of the data-related operating arrangements and policy requirements for their data assets either directly or via appointed representatives • Creation and Maintenance of [3]Data Inventory documents [1]Approval for Data Request pertaining to Marketing Campaign or Servicing Campaign purpose will be by Executive Director of Marketing or Group Head of BCM – refer to Group Data Management Policy Section 3.3 The use of the data, for any purposes other than Marketing Campaign or Servicing Campaign, would require staff to seek approval from the respective Data Owner [2]Data Quality procedures are explained in Group Data Management Policy Section 2.3 [3]Data Inventory is explained in Group Data Management Policy Section 3.2
Data Protection Officer	Extract @ 27 Jul 2022 from Group Privacy Policy – Section 3.3 Each Data Protection Officer (“DPO”) is a member of the Group Business / Function and is responsible for: a) Informing and advising their respective Business / Function on its Privacy obligations; b) Ensuring that relevant standards / procedures / manuals owned by their respective Business / Function are aligned with the requirements as set out in this policy and related standards; c) Monitoring and reporting compliance with the Privacy obligations within their respective Business / Function to Group Privacy Compliance, being the Group DPO; d) Providing advice and guidance on Privacy obligations in the Data Protection / Privacy Impact Assessments for their respective Business / Function and escalated in line with the Data Protection / Privacy Impact Assessment process;

Role	Responsibilities
	e) Providing advice and guidance on and handling Personal Data Breaches for their respective Business / Function escalated in line with the criteria set out in the Data Incident and Breach Management Standard; f) Reporting to Group Privacy Compliance any Privacy risk which could cause a material impact on the Group; g) Handling privacy related questions/complaints for their respective Business / Function from employees and anyone else covered by this policy; h) Dealing with requests for their respective Business / Function from individuals to access the Personal Data or other information that the Group holds about them; i) Reviewing and approving any contracts / agreements for their respective Business / Function with third parties that may handle Personal Data; and j) Maintaining a list of the various Personal Data collection processes for their respective Business / Functions to ensure that all aspects of Personal Data processing are well monitored and addressed
Department Data Representatives	• Serve as representatives from their departments / teams in the data risk forum, as well as the liaison person between the departments / teams and data risk team. • Communicate any key requirements and/or messages from the data risk forum back to their departments / teams.
Data Stewards	Essential in the implementation of Framework and Policy set by Group Risk team. Each Data Steward is assigned to specific Data Owners/Business Functions to work collaboratively in achieving data management goals. Responsibilities include the following: • Collaborate with the Data Owner and Group Risk to ensure robust Data Quality management and establish best practice-based processes, procedures, policies, and standards. • Ensure management of data issues which includes tracking, escalation and resolution by Data Owner • Propose and implement Action Plans to address Data Quality issues with support from the Technology team. Data Steward is appointed from Data Science and Analytics (DSA) team

Second Line of Defence

Role	Responsibilities
Group Risk Team	• Sets the overall data governance and management strategy to manage the Group's data risk in accordance with the Group's Risk Management Framework and appliable laws and regulations. • Designs and regularly reviews the data risk governance framework and data management policy. • Supports the Group CRO in leading the implementation of proper data risk governance and data management across the Group in accordance with this Framework. • Oversees the management of critical data and personal data held within the organisation's possession. • Reviews data management risk in relation to products, channels, transactions and counterparties. • Conducts annual audit on departments to ensure that data protection practices comply with the requirements of the data protection certifications on a sampling basis.
Tech Risk Team	• Oversees governance of technology and processes to address overall information security risks. • Provides feedback on the information security policy. • Provides second line reporting on the effectiveness of information risk posture or activities to the ORC.
Privacy Compliance Team	• Oversees and provide advice in the regulatory requirements relating to data privacy and data protection. • Designs and regularly reviews the data privacy policy. • Reviews privacy risk in relation to products, channels, transactions and counterparties.

Third Line of Defence

Roles	Responsibilities
Internal Audit	▪ Assess and report on the effectiveness of the design and operation of the framework of controls which enables risk to be assessed and managed.

Roles	Responsibilities
	• Assess the effectiveness of the management actions to address deficiencies in the framework of controls and risks that are out of tolerance.

3. Data Management

3.1 Critical Data and Personal Data

While the Group processes a huge amount of data, the focus of this Framework is predominantly on the following categories of data:

a. **Critical Data** – Defined as 'Confidential' or 'Secret' data (classified in accordance with the Group's Information Classification Document) with the potential of Moderate, Major and Very Severe impact as per the Integrated Assurance Framework ("IAF").

b. **Personal Data** – Personal information or personally identifiable information ("PII"). As defined under the Personal Data Protection Act ("PDPA"), personal data refers to data about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access.

The relationship between Critical and Personal Data is illustrated in Figure 2

Figure 2

3.2 Data Lifecycle Management

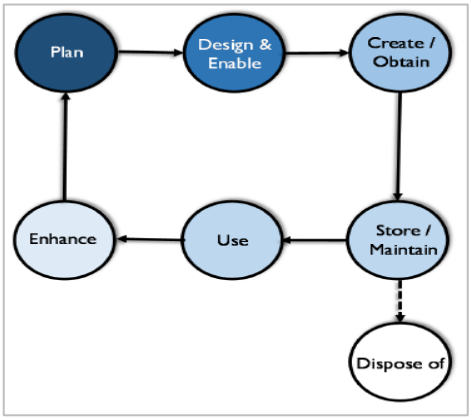

Figure 3: Data Lifecycle
(Extracted from DAMA DMBOK 2nd edition)

Effective data management includes understanding how data traverses throughout its life from the time it is created or obtained to its eventual disposal (refer to Figure 3 for an illustration of the data lifecycle).

In addition, data is rarely static as it moves along the lifecycle, and may be cleansed, transformed, merged, enhance, or aggregated. These are internal iterations within the data lifecycle that while not captured in Figure 3, should be duly considered when managing data.

The following provides a general description of the key stages in the data lifecycle.

a. **Plan/Design & Enable**: Avoid over collection of data by creating a plan which defines and captures data that is relevant to the defined purpose. In addition, the plan should include the design of how the data should be created or obtained.

b. **Create / Obtain**: Data is generated by the Group or obtained from customers or third parties. Each policy / account application, staff hire, communication and interaction either creates or obtains data.

c. **Store / Maintain**: As data is created or obtained, it needs to be stored for subsequent use. This could either be in the form of physical storage or through the creation of databases or data lakes whether maintain on-premise or via clouds. Regardless of storage forms, protection with the appropriate level of security should be applied alongside considerations on backup and recovery processes.

d. **Use / Enhance**: Depending on the objective and outcome, data can either be used directly or through a processing stage where it is enhanced for data users to perform analysis and other authorised purposes.

e. **Dispose of:** Data is destructed or purged which entails the removal of every copy of a data item. This ensures compliance with regulatory retention obligations.

The Data Inventory and related documents record the Critical and Personal Data collected and/or processed by the company as it moves throughout the data lifecycle. Each department will maintain a copy of their Data Inventory documents which comprises the Data Inventory, Data Map, Records Retention Schedule, Disposal Schedule and Consumer Log. These will be reviewed and updated annually with oversight by the Group Risk team.

Data Security is expected to be managed throughout the data lifecycle to ensure that data is secure, and the risks associated at each data life stage is mitigated.

4. Data Risk Management Process

4.1 Definition of Data Risk

Data risk can be explained as the exposure to loss of value, financial or reputation caused by issues or limitations to an organisation's ability to acquire, store, protect, transform, move, and use its data assets, such as weak governance, data breaches, inaccurate or bad quality data, misalignment, lack of documentation, dark data and unethical use of data.

4.2 Data Risk Appetite

The Group's risk appetite framework outlines the risks that the Group selects and manages in the pursuit of return, the risks the Group accepts but seeks to minimise and the risks the Group seeks to avoid or transfer.

For data risk, the relevant risk preference statements are:

i. The Group has no appetite for conducting business in a way where individuals' personal data are used for unauthorised or unethical manners; and

ii. The Group has no appetite for intentional or repeated breaches of law, regulation or policy. Recognising that risk events of this nature will occur, the Group will, to limited degree, tolerate accidental data breaches.

The data risks tolerances with respect to the three pillars: data management, data privacy and information security, shall be maintained in accordance to the Integrated Assurance Framework ("IAF").

The Data Risk Team shall report to the ORC if the data risk tolerances have exceeded the defined tolerance set in the respective policies.

4.3 Data Protection Impact Assessment ("DPIA")

It is a requirement for risk, including data risk, to be considered in key business decisions. The Group Risk and Privacy Compliance team should be involved upstream in material projects, activities, processes, systems, vendors and products, to evaluate the potential data risk exposures and controls. This is to enable the Group Risk and Privacy Compliance, as the second line of defence, to perform its role of reviewing the completeness and accuracy of data risk identification, measurement and management, and the adequacy of, and progress against, mitigation.

The DPIA helps to assess if the handling of Personal and Critical data complies with the data protection regulations and best practices and facilitate the design of appropriate technical or process control measures to safeguard against data protection risks. More information is available in the DPIA document.

5. Data Incident and Data Breach

A Data Incident is the violation of the Group's policy and guidelines that results in the compromise of the data being held in the company's possession.

A Data Breach, as defined in the Personal Data Protection Act ("PDPA") in relation to personal data, refers to any unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data. It also includes the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

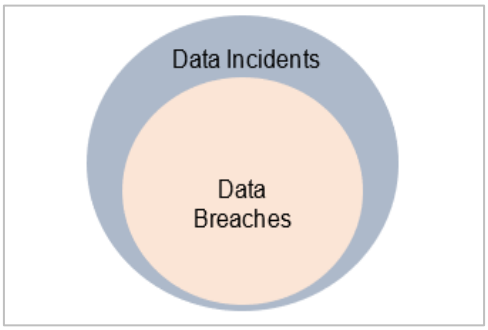

Figure 4: Data incidents and Data Breaches

Figure 4 illustrates the relationship between Data Incidents and Data Breaches.

All businesses must comply with the Data Incident and Breach Management Standard issued by the Group Risk function. This ensures that there is a clear plan to respond to Data Incident and/or Data Breach and comply with regulatory requirements.

It should be noted that there are different laws with different notification and reporting requirements for Data Breaches. In particular, the Group is required to comply with the notification and reporting obligations to the Monetary Authority of Singapore ("MAS") and the Personal Data Protection Commission ("PDPC").

6. Framework, Policies and related documents

This Framework will be supported by the following policies ("Policies") which sets out the expectations of this Framework in greater details.

Policy	Policy Owner
Group Data Management Policy	Group CRO
Group Privacy Policy	Privacy Compliance
Singlife Information Security Policy	Group CISO

This Framework should be read in conjunction with the following documents:

- Group Risk Management Framework
- Integrated Assurance Framework Guidance
- Technology Risk Management Framework
- Group Data Management Policy
- Singlife Information Security Policy
- Group Privacy Policy
- Data Incident and Breach Management Standard
- Data Inventory and related documents
- Singlife Information Security Standard

The companies within the Group and their respective departments must ensure that their framework, policies, standards, guidelines and procedures are consistent with this Framework.

7. Review

This Framework will be reviewed at least once annually or when there is a major change, with changes approved by the Group CRO and the ORC. Where no changes to the Framework are proposed after the annual review, the ORC must still be informed that a review has been conducted.

8. Non-compliance

Non-compliance or any identified issues that could lead to non-compliance must be:

- Notified to Group Risk team and Group CRO; and
- Rectified immediately or within a reasonable timeframe agreed with the Group CRO