Enterprise Risk Management Framework

September 2022

Document Name:	Enterprise Risk Management Framework
Approver:	Link Group Board of Directors (**Board**)
Executive Sponsor:	General Counsel and Company Secretary
Policy Owner (Author):	Global Head of Enterprise Risk Management
Approval Date:	November 2021
Review Frequency:	Every two years unless required more frequently
Last Review Date:	November 2021
Next Review Date	November 2023
Contact for Questions:	Chris Karatasas, Head of Framework, Policy & Training, Enterprise Risk
Information Security Document Classification	Confidential *Refer to the Link Group Information Classification and Handling Policy*

Contents

1. Overview

1.1 Purpose

The Enterprise Risk Management Framework (ERMF) sets the strategic approach for managing risk by defining standards, objectives and responsibilities for all areas of the Group. It supports management in effectively managing its risks and developing a strong risk culture. The framework sets out:

- segregation of duties utilising a Three Lines of Defence model;
- the identification, management and reporting of risks;
- risk appetite requirements, which define the types and level of risk the Group is willing to undertake in the pursuit of its business strategy; and
- roles and responsibilities for managing risk and the accountabilities of the Executive Management, including Divisional Chief Executives, as well as Link Group committees.

It describes the Group's approach for managing the material risks it faces. This helps the Board and management answer pertinent questions facing the Group, including questions around the risks to our business strategy; our appetite relating to material risks; our approach to controlling, monitoring and managing these risks; and how we respond to possible scenarios that could impact Link Group.

The Board is ultimately responsible for our ERMF and the oversight of its operation by management. The Board has delegated the oversight of the Framework and its implementation to the Global Head of Enterprise Risk Management as the Accountable Executive. Business Divisions and Group Functions are accountable for implementing, and monitoring adherence to the Framework.

1.2 Application

The ERMF applies to all employees within Link and its subsidiaries, referred to collectively as the "Link Group" (defined in this document as 'Link', 'Group', 'we' or 'our').

Exceptions to the ERMF are not permitted. If a subsidiary or local entity needs to develop additional requirements to meet local conditions, regulatory or legislative requirements, these can be included as an addendum to the Framework. The person responsible for the ERMF in the subsidiary or local entity must first consult with the Global Head of Enterprise Risk Management.

1.3 Enterprise Risk Management Framework document responsibilities

We have documented frameworks, policies, standards and procedures in place to manage each type of risk we take. These are established, maintained and embedded at Group, Divisional and regulated legal entity levels for the management of risk and decision making.

Our risk management documents are subject to periodic review to confirm they remain effective and appropriate, to promote consistency and clear decision making. Document owners are accountable for their documents through the document lifecycle.

The biennial review and approval of the ERMF by the Board ensures that it continues to remain sound, fit for purpose, and aligns to the Group's purpose, business strategy and risk appetite with consideration to the external and internal environments.

Global Head of Enterprise Risk Management can make non-material changes to the ERMF, e.g., changes that have been approved in other Board or Board Committee papers and need to be reflected in this document. Non-material changes are those that do not change the fundamental operation of the document.

Breaches of the ERMF must be escalated to the Global Head of Enterprise Risk Management within two business days for action and escalation as appropriate. All breaches must be recorded and managed in line with the Incident Management Policy.

Regulated subsidiaries and legal entities in the Group may be expected to maintain risk management documents for their specific entity in order to comply with local regulatory or statutory requirements. In such circumstances, Link Group documents must be used as the basis for entity-specific documents with changes only permitted to align or comply with local regulatory requirements. The boards of these entities are responsible for oversight and management of the risks relevant to that entity and for the approval of the associated key risk documents, with appropriate oversight by Group.

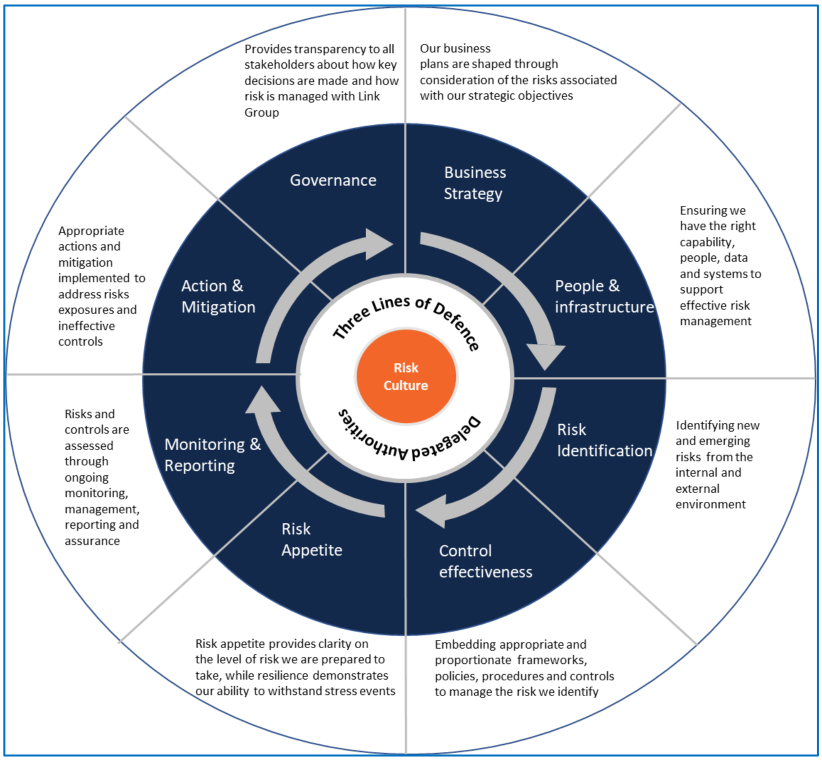
Procedures are established in the First and Second Lines to support the implementation and operating effectiveness of these frameworks, policies, and standards. Controls are established and periodically reviewed to verify they remain fit for purpose and operate effectively to manage and monitor risk.

2. Framework Components

Our ERMF comprises of eight components underpinned by a strong risk culture and Three Lines of Defence model, shown in Diagram 1. These components operate independently as well as interactively to provide a complete approach for managing risk. Irrespective of how effective the components are in principle, they cannot be relied upon in the absence of a strong risk culture and an effective Three Lines of Defence model.

The components are reviewed individually and collectively each year to confirm the operating effectiveness of the framework and ongoing compliance with internal and external regulatory and statutory obligations.

Diagram 1: Enterprise Risk Management Framework components


Provides transparency to all stakeholders about how key decisions are made and how risk is managed with Link Group
Our business plans are shaped through consideration of the risks associated with our strategic objectives
Governance
Business Strategy
Ensuring we have the right capability, people, data and systems to support effective risk management
Appropriate actions and mitigation implemented to address risks exposures and ineffective controls
Action & Mitigation
People & infrastructure
Three Lines of Defence
Risk Culture
Delegated Authorities
Risks and controls are assessed through ongoing monitoring, management, reporting and assurance
Monitoring & Reporting
Risk Identification
Identifying new and emerging risks from the internal and external environment
Risk Appetite
Control effectiveness
Risk appetite provides clarity on the level of risk we are prepared to take, while resilience demonstrates our ability to withstand stress events
Embedding appropriate and proportionate frameworks, policies, procedures and controls to manage the risk we identify

2.1 Risk Culture

Risk culture can be defined as the customs, attitudes and behaviours related to risk awareness, risk taking and risk management. This is reflected in how the Group identifies, escalates and manages risk matters.

Risk culture and capabilities are critical to ensure that staff can fulfil their risk-related obligations efficiently and effectively, and that Link Group operates within its risk appetite. At Link Group, all employees are responsible for strengthening Link Group's risk culture.

A strong risk culture is essential for effective risk management as it promotes individual and organisational risk awareness and accountability, encourages employees to speak up and provides a safe environment for them to do so, and shapes behaviours and judgements to support sound decision making and risk-taking. A strong risk culture continuously improves risk practices, ensuring key learnings and experiences are integrated into Group-wide and stakeholder outcomes. A strong risk culture also ensures that emerging risks and risk-related behaviours are within risk appetite. Those risks that are outside of appetite are recognised, assessed, escalated, and addressed to return within appetite in a proactive and responsive way.

2.2 Three Lines of Defence

We have adopted the Three Lines of Defence Model to set clear boundaries in which all employees play an active role in managing risk. This provides clear roles, responsibilities and accountabilities across the Three Lines of Defence.

Our Three Lines of Defence Model is aligned to the eight components of our ERMF and applies to all Link Group employees. The key principles underpinning the Three Lines of Defence Model are:

- Business ownership and management of the risks they originate and operation of controls to mitigate them.
- Risk Management's ownership of the Three Lines of Defence Model.
- Flexibility to account for future needs and changes in the operating environment.
- Low tolerance for deviations from our Three Lines of Defence Model
- Efficiency and effectiveness in interactions between and within the Lines of Defence; and
- Clearly articulated relationships and no duplication in activities or shared primary accountability.

The delineation and responsibilities between the Three Lines of Defence are:

- The **First Line of Defence** is the Business - all employees engaged in the revenue generating and client-facing areas of the Group and all associated support functions. The first line is responsible for identifying, assessing, and managing the risks they generate, establishing effective controls, identifying and managing incidents and ensuring they meet their compliance obligations.

- The **Second Line of Defence** is comprised of the Risk and Compliance function. The role of the second line is to establish the frameworks and policies to support the business in identifying, assessing, and managing their risks and regulatory compliance obligations as well as limits, under which first line activities shall be performed, consistent with the risk appetite of the Group. Risk and Compliance also provide guidance, challenge and independent oversight of the first line.

- The **Third Line of Defence** is Internal Audit, who are responsible for providing the Board Audit Committee with independent assurance over the effectiveness of the Group's governance, risk management and control practices.

- All employees are responsible for managing risk. Leaders have additional responsibilities commensurate with their positions.

2.3 Delegations of Authority

Link Group's Delegations of Authority Policy sets out the authority that the Board has delegated to the Chief Executive Officer (CEO) & Managing Director to operate the business on a day-to-day basis. The Policy also sets out the authority that the CEO & Managing Director has in turn delegated to members of the Executive Leadership Team (ELT) to operate their businesses and functions in an efficient and effective manner. The delegated authorities allow specified individuals to commit Link Group to transactions, expenditures and various decisions while providing good governance principles to guide appropriate and responsible exercise of that authority.

2.4 Business Strategy

Our business strategy is shaped through considering the risks associated with our strategic objectives. Our strategic priorities are set taking into consideration our purpose, values and risks associated with the Group's strategy and business plans, and the impact our strategic objectives and business plans may have on our risk profile. In formulating our business strategy, we also consider developments in the external environment, emerging risks, regulatory requirements and stress testing outcomes.

The board strategy review outlines the strategic priorities for the Group and considers the impact our strategic objectives and business plans may have on our risk profile. The CEO and ELT define the Group's business strategy, in consultation with, and subject to approval by the Board. The ELT is responsible for establishing and managing long-term strategies and shorter-term priorities for their areas of responsibility and for ensuring such strategies are aligned with the Group's overall strategic priorities and risk appetite.

The Risk and Compliance function provides oversight of the Group's strategic risk by providing independent review of these processes and independently monitoring and reporting on the assessed level of risk against our risk appetite metrics.

2.5 People and Infrastructure

Ensuring we have appropriate management capabilities to effectively carry out our assigned roles and responsibilities is a core part of our ERMF.

Each Line of Defence is responsible for confirming they have appropriate resources and capabilities to manage risk. This includes:

- Resources that are sufficient in number and with the right skills;
- Role descriptions with clear accountabilities and responsibilities linked to the Group's remuneration and disciplinary requirements;
- Training and development, including formal training, workshops and on-line learning; and
- Data, systems and tools to support effective risk identification, assessment, and management, clear decision making and compliance with internal and external obligations.

2.6 Risk identification and assessment

We identify risk as part of normal business operations, in response to changes in our business strategy, internal operating priorities and projects and in the external environment. All employees are responsible for identifying risks that occur within their day-to-day responsibilities, documenting them in the Group's GRC system and taking appropriate action to manage those risks. Identifying, understanding, and communicating these risks inform risk appetite and the management of risk.

We regularly assess our operating environment to highlight existing and emerging risks that could have a significant impact on Link Group's risk profile and its ability to meet its strategic objectives. An emerging risk is a developing risk that could in the future materially impact our financial results, reputation, business model or strategy. It is distinguished by the lack of clarity in respect to the probabilities, impacts, timing, and/or ranges of potential outcomes.

Leading risk indicators are forward-looking metrics that help to identify potential heightened areas of concern or decreasing control effectiveness before a risk incident occurs. Leading indicators are usually linked to risk cause(s) or preventative controls and are used in conjunction with other management judgements of regulatory, economic and business conditions impacting the Group's risk profile. Early identification of changing risk profiles enables management to proactively focus on issues of concern as they emerge.

Our assessment of existing and emerging risks is used to develop action plans and stress tests related to our exposure to certain events. These practices support the maintenance of a forward-looking risk assessment by management. Risks are identified, analysed and discussed by senior management. Mitigation plans are prepared, monitored and adjusted as required.

Consideration of the broader internal and external risk environment in parallel with key risk analysis improves cross-divisional and cross-risk identification. This helps inform future risk-related initiatives and the prioritisation of remediation projects and resource allocation.

2.7 Control effectiveness

A control is any action taken by management that either reduces the likelihood of a risk occurring or reduces the potential impact from that risk. Controls are considered key when they are critical to mitigating the risk or are mandated as part of regulatory and legislative compliance.

Key controls are documented in the Group's GRC system. Controls are assessed for both design effectiveness and operating effectiveness as part of the Group's Control Self-Assessment process.

In line with the Issues and Actions Management Policy[1], where controls are not assessed as effective, issues must be raised and accompanied by actions to remediate control deficiencies to acceptable levels and within stipulated timeframes. Key controls must be assessed for design effectiveness and operating effectiveness at least annually.

2.8 Risk appetite

Risk appetite is defined as the level and type of risk the Group is willing and able to take given its business strategy and obligations to stakeholders. It provides a basis for ongoing dialogue between management and Board with respect to the Group's current and evolving risk profile, allowing strategic and financial decisions to be made on an informed basis.

Risk appetite takes into account the objectives of our key stakeholders, e.g., the interests of customers, employees, the community, shareholders, and regulators' expectations and requirements. In setting risk appetite, we are guided by our need to balance the different objectives of our stakeholders.

Risk Appetite Statements are used to articulate the types and levels of risk Link Group is willing to take. The Group Risk Appetite Statement includes qualitative statements and quantitative measures which provides a reference for risk taking across the Group, providing clarity of our risk appetite and risk-taking capacity for our material financial and non-financial risks. They also allow us to measure our risk profile against our stated risk appetite. The Group Risk Appetite Statement is approved by the Board annually. It is a strategic document intended to support long-term value creation and execution of our business plans and strategic objectives.

The Group Risk Appetite statements and metrics may be cascaded to more granular levels within the organisation to provide a structured approach for decision making within approved limits. Divisions and regulated entities, where required, are responsible for setting Management Risk Appetite Statements in the context of specific business strategies and objectives, while aligning to the Group Risk Appetite Statement. Developing, approving and operating within the Group and relevant Management Risk Appetite Statements is a core responsibility of the Business.

Risks outside of appetite are subject to heightened monitoring and remediation and reporting to the relevant Board and management committees.

[1] The Issue & Action Management Policy is currently in development.

2.9 Monitoring and Reporting

Risk and control management

Risk and control management is used across the Group for the identification, assessment, management, monitoring and reporting of risks and controls. Risks are identified and measured, taking into consideration financial and non-financial impacts. This monitoring process is an input into the construction of risk profiles at Group and Divisional levels, which include an assessment of residual risk – the actual risk remaining after control activities are put in place.

The First and Second Lines are accountable for monitoring the risks, controls and compliance obligations related to their activities and operations and for monitoring adherence to risk management policies and standards.

Incident Management

Our Incident Management Policy describes the requirements and process to identify, record, escalate, rectify, report and close out events. Incidents are classified based on their actual or potential customer, financial, staff, regulatory or reputational impact.

Everyone is responsible for identifying and reporting incidents. The early identification, reporting, and escalation of potential or actual incidents enables the Group to minimise losses and any associated customer, regulatory, or reputational impact. Where we do not get it right, we look to remediate in a timely manner.

Breach Management

When policies, risk limits, or regulations are not adhered to, breaches can occur. The requirements for management of breaches are outlined in policies of the Group. Where required, notifications are provided to the Group Board or Board Committees, regulated entity boards, and regulators regarding any significant breach of policy or regulation, including material deviations from the ERMF and its components. Accountability for compliance with Link Group's obligations, including supporting the identification, management and reporting of breaches policies, frameworks, and standards rests with the First Line of defence. Risk and Compliance is responsible for reporting breaches to the Group Board or Board Committees, regulated entity boards and regulators.

2.10 Action and Mitigation

Action plans are designed and appropriately implemented to manage all our identified risks to ensure we remain within our approved risk appetite or return out of appetite risks to within appetite.

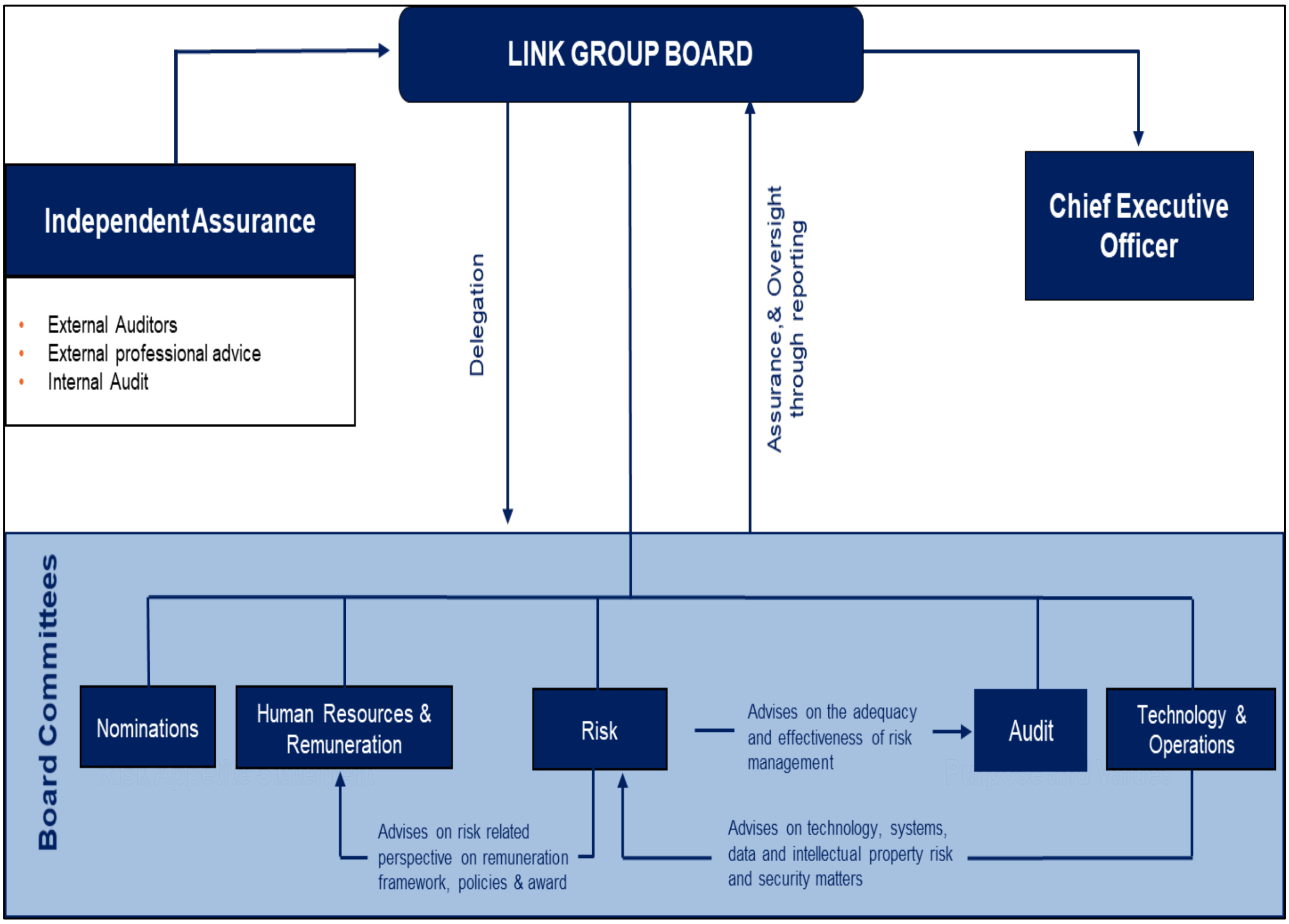
In managing our actions, we aim to be both timely and deliberate. This includes implementing remediation plans that are clear and well-defined, with measurable milestones and tracking of deliverables.

We have a strong focus on continuously improving the way we manage risks by responding to opportunities to improve the management of identified risks. This includes enhancing our risk management documents and controls in conjunction with their periodic review or from issues self-identified or independently raised.

2.11 Governance

Our ERMF is supported by formal committees and other governance fora where data, analysis and recommendations are escalated appropriately and on a timely basis to support decision making. This is shown in Diagram 2 below.

Board Committee structure


LINK GROUP BOARD
Independent Assurance
External Auditors
External professional advice
Internal Audit
Delegation
Assurance,& Oversight through reporting
Chief Executive Officer
Board Committees
Nominations
Human Resources & Remuneration
Risk
Advises on the adequacy and effectiveness of risk management
Audit
Technology & Operations
Advises on risk related perspective on remuneration framework, policies & award
Advises on technology, systems, data and intellectual property risk and security matters

Note: Arrows denote escalation paths from and to various Committees charged with overseeing Link Group's risk.

There are two Board-level forums which oversee the application of the ERMF and review and monitor risk across the Link Group. These are: Link Group Board Risk Committee and the Link Group Board Audit Committee.

Link Group Board Risk Committee:

In addition to supporting the Board in setting the risk appetite of the Group, the Board Risk Committee is responsible for:

- reviewing risk management and compliance frameworks and policies, and monitoring the effectiveness of their implementation;
- monitoring the Group's risk profile against the agreed appetite. Where actual performance differs from expectations, the actions taken by management are reviewed to ascertain that the committee is comfortable with them.

Link Group Board Audit Committee:

The Audit Committee receives and considers reports from the Risk Committee on the adequacy and effectiveness of the Company's risk management, internal compliance and control systems and the process and evidence adopted to satisfy those conclusions. The Committee is also responsible for reviewing whether the Company has any material exposure to any economic, environmental and social sustainability risks and for reviewing and monitoring related party transactions and investments involving the Company and its directors.

Further, there are two other Board-level committees which oversee the implementation of key aspects of the Framework:

Link Group Technology and Transformation Committee:

The Technology and Transformation Committee assists the Board with overseeing management's development and implementation of the Company's technology strategy, capability, architecture and execution with a focus on digital transformation, data and cyber security. It is also responsible for reviewing emerging innovations in technology and trends for potential application within the Company; and monitoring the Company's information system and related data management risks, and the effectiveness of the associated controls.

Link Group Board Human Resources and Remuneration Committee:

The Human Resources and Remuneration Committee is responsible for oversight of the human resources strategy and supporting policies and practices for the Company's employees and directors and oversight of the policies and practices of the Company regarding the remuneration of directors and other senior executives and reviewing all components of the remuneration framework; this includes receiving information on risk management performance and proposals on risk adjustments to variable remuneration.

Divisional Risk Committees

Divisional risk committees support the Group to effectively identify, evaluate, monitor and manage all key risks within the relevant Division, with appropriate Second Line input and oversight.

These committees are responsible for:

- Overseeing the embedding of the ERMF and other risk related management frameworks and key supporting policies
- Monitoring the division's risk profile and management of identified risks;
- Identifying key emerging and strategic risks for the division and allocating responsibility for assessing their impact and responding as appropriate;
- Supervising the rectification of risk issues identified in the division, including any associated action plans;
- Overseeing the response to significant regulatory matters, reviews and investigations in relation to the division; and
- Actively managing key risk issues with potential Group-wide, cross-divisional or multi risk class impacts.

Divisional risk committee must refer material matters, including emerging risks or issues, to appropriate decision-making authorities for consideration.

Regulated Subsidiary or Entity Level Risk Committee

Regulated subsidiary and entity level risk committees support the Group to effectively identify, evaluate, monitor and manage all key risks within the relevant subsidiary or entity with appropriate Second Line input and oversight.

These committees are responsible for:

- Monitoring the risk profile and management of identified risks;
- Identifying key emerging and strategic risks and allocating responsibility for assessing their impact and responding as appropriate;
- Supervising the rectification of risk issues identified, including any associated action plans;
- Overseeing the response to significant regulatory matters, reviews and investigations in

relation to the division; and

- Actively managing key risk issues with potential Group-wide or multi risk class impacts.

A regulated subsidiary and entity risk committee must refer material matters, including emerging risks or issues, to appropriate decision-making authorities (including Board Risk Committee) for consideration.

3. Risk Documentation Hierarchy

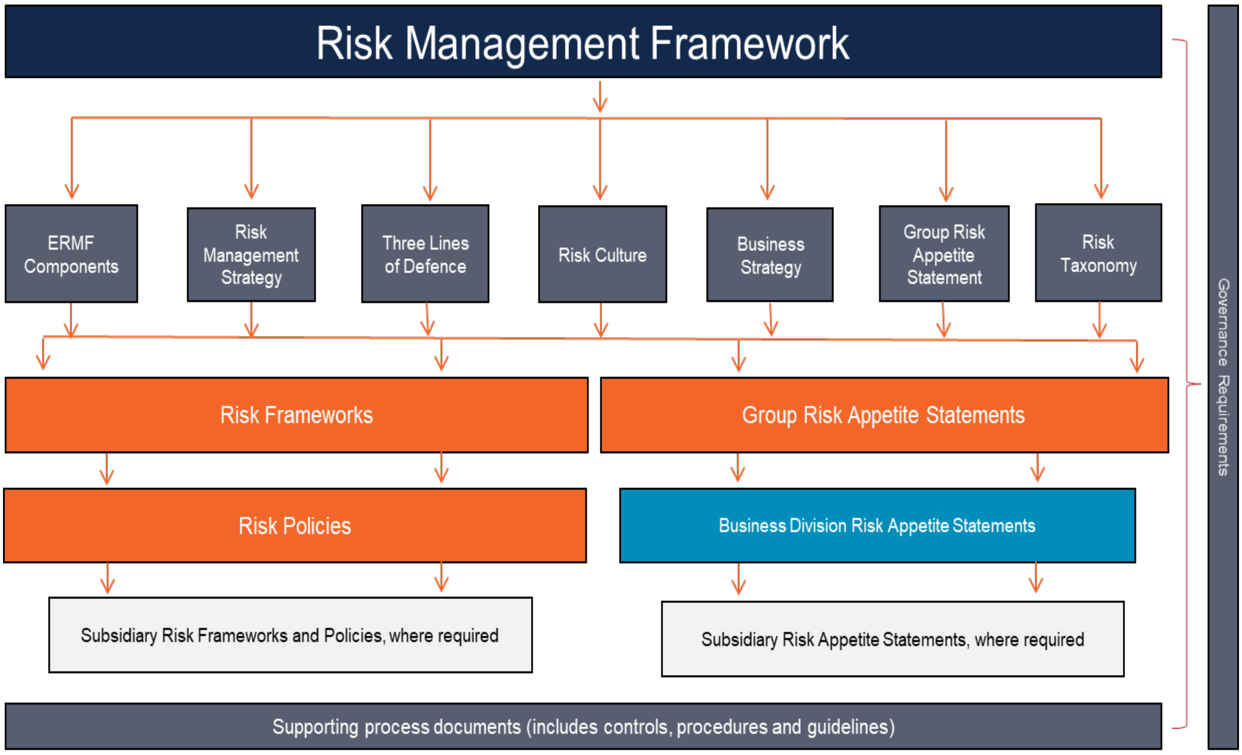
Each ERMF component is supported by formal documentation which provides a structured approach to meeting our internal and external obligations, operating within our approved risk appetite and effectively managing risk.

Our risk documentation hierarchy is the aggregation of the documents which support our ERMF. This hierarchy is shown in Diagram 3 and indicates the linkages between these documents to enable effective understanding and management of risk across the Group. Each document describes the approach for managing a particular risk class (or type of risk), activity or process for one or more of the framework components.

This ERMF document is the overarching risk document for Link Group.

An individual document's purpose, scope, level of details and approval requirements determines where it is placed in the hierarchy. All relevant documents must align to and comply with their relevant parent documents and ultimately to the ERMF without duplication or inconsistencies. To facilitate this, documents such as risk class[2] frameworks should reference key supporting policies and related documents.

Diagram 3: Risk document hierarchy


Risk Management Framework
ERMF Components
Risk Management Strategy
Three Lines of Defence
Risk Culture
Business Strategy
Group Risk Appetite Statement
Risk Taxonomy
Risk Frameworks
Group Risk Appetite Statements
Risk Policies
Business Division Risk Appetite Statements
Subsidiary Risk Frameworks and Policies, where required
Subsidiary Risk Appetite Statements, where required
Supporting process documents (includes controls, procedures and guidelines)
Governance Requirements

[2] A risk class represents a type of risk that the Group has a material exposure to.

4. Requirements

4.1 Corporate governance requirements

The ERMF supports compliance with the corporate governance principles and legislative requirements outlined in Link Group's Corporate Governance Statement.

The Corporate Governance Statement summarises our corporate governance framework, policies and practices including the accountabilities, roles and responsibilities of the Board, Board Committees and management.

4.2 Regulatory Disclosures

Materiality or significance considerations are applied to all compliance incidents in relation to regulatory notification obligations and voluntary disclosure. These considerations and our notification obligations are governed by the Link Group Regulator Interaction Policy.

When assessing matters to determine whether regulators are notified, Link Group prioritises timely notification and transparency over ensuring the completeness and certainty of our inquiries. This applies to all types of notification. Link Group seeks to comply with its notification obligations, and in doing so, aims to maintain an open and transparent relationship with its regulators.

5. Document change history

Amendment Number	Approved by	Date	Description of changes
N/A	TBA	November 2021	New version
1	Chief Risk Officer	July 2022	Section 2.2 updated to align with the Three Lines of Defence Model Standard
2	Global Head of Enterprise Risk Management	September 2022	To remove references to the Chief Risk Officer (CRO) and Executive Risk Committee (ERC)