



ENTERPRISE RISK MANAGEMENT FRAMEWORK

Version No	7.1 (refer to C7 in Part C for more details)
Framework Owner Name	Sadia Ricke
Framework Owner Job Title	Group Chief Risk Officer
Framework Contact Name	Ioana Cornisteanu
Framework Contact Job Title	Head, Strategic Risk Management and Governance
Business Scope	All Businesses, except those outlined in Part A, Section 1.4
Function Role	All Functions
Geography Scope	Global
Approval Date	19 Dec 2024
Effective Date	23 Dec 2024
Next Review Date	31 Jul 2025

For queries and questions, please email 'FrameworkandPolicyManagement.ERM@sc.com'
Additional contacts: Ioana.Cornisteanu@sc.com, Renzo.Baio@sc.com

Table of Content

	Part A – Main Chapter	Page
1	Introduction and Purpose	4
2	Risk Culture	4
3	Conduct Risk Management	4
4	Three Lines of Defence	5
5	Source of Authorities	6
6	Committees and Meetings	7
7	Principal Risk Types	8
8	Role and Responsibilities – Control Model	9
9	Group Strategy and Strategic Risk Management	16
10	Group Risk Appetite Framework	17
11	Enterprise Risk Identification, Assessment, Mitigation and Monitoring	19
12	Enterprise Stress Testing	20
13	Risk Reporting, Risk Data Aggregation and Data Quality	21
14	Validation, Effectiveness Review, and Independent Assurance	21
15	Country Risk	22
16	Risk Management for Branches and Subsidiaries	22
	Part B - Risk Type Frameworks	
1	General Principles and Governance	26
2	Treasury Risk Framework	29
3	Credit Risk (CIB) Framework	41
4	Credit Risk (WRB) Framework	57
5	Traded Risk Framework	65
6	Compliance Risk Framework	74
7	Financial Crime Risk Framework	83
8	Operational and Technology Risk Framework	90
9	Model Risk Framework	98
10	Environmental, Social and Governance and Reputational Risk Framework	107
11	Information and Cyber Security Risk Framework	119
	Part C – Common Appendices	
C1	Risk Taxonomy	136
C2	List of Group Policies	136
C3	List of Priority Reports	138
C4	Group Risk Assessment Matrix	144
C5	List of Group Standards tagged to Frameworks	145
C6	List of Processes and Controls	146
C7	Change Log	146
C8	List of Abbreviation and Terms	150

Part A

Main Chapter

Main Chapter

1. Introduction and Purpose

- 1.1 The **Enterprise Risk Management Framework** (ERMF or this Framework) sets out the principles and minimum requirements for risk management and governance across the branches and subsidiaries of **Standard Chartered PLC** (the Group).
- 1.2 This Framework aligns with the Risk Control chapter of the **Prudential Regulation Authority** (PRA) Rulebook requirements for UK registered banks.
- 1.3 The Group **Board of Directors** (Board) will approve this Framework as part of the annual review and any ad hoc material changes. The **Group Chief Risk Officer** (GCRO) has the authority to make temporary or non-material changes to Part A of this Framework and material changes to the **Risk Type Frameworks** (RTFs) included in Part B. The **Risk Framework Owners** (RFOs) have the authority to make non-material changes to the RTF for which they are responsible.
- 1.4 **SC Ventures**¹ (SCV) is required to operate within the Group **Risk Appetite** (RA), however, SCV is out of scope of the requirements outlined in this Framework and has a separate Risk Management Framework aligned to the Group ERMF.

2. Risk Culture

- 2.1 Risk management is at the heart of banking, it is what we do. Doing it effectively is how we drive commerce and prosperity for our clients and our communities, and it is how we grow sustainably and profitably as an organisation.
- 2.2 Risk culture encompasses our general awareness, attitudes, and behaviours toward risk, as well as how risk is managed enterprise wide.
- 2.3 A healthy risk culture is one in which everyone takes personal responsibility to identify and assess, openly discuss, and take prompt action to address existing and emerging risks. We expect those in our control functions to provide oversight and challenge constructively, collaboratively, and quickly.
- 2.4 This is not a static state – the risks we face constantly evolve, and we must always look for ways to manage them as effectively as possible. We will not always get it right, and unfavourable outcomes will occur from time to time. A healthy risk culture means that we react in those situations quickly and transparently and take the opportunity to learn from our experience and formalise what we can do to get better.
- 2.5 Every bank should strive to promote a healthy risk culture, but it is particularly important for us because it enables us to safely harness the power of our unique diversity across some of the world's most dynamic markets for the benefit of our people, clients, and communities. This effort is reflected in our valued behaviours, underpinned by our Code of Conduct and Ethics, and reinforced by how we hire, develop, and reward our people, serve our clients, and contribute to communities around the world.

3. Conduct Risk Management

- 3.1 Conduct Risk is defined as the *“Risk of detriment to the Group’s clients, investors, shareholders, counterparties, employees, as well as to market integrity and competition arising from (i) the activities performed by the Group, or (ii) individual behaviour and actions including instances of wilful or negligent misconduct”*.
- 3.2 It is critical to manage Conduct Risk to deliver good outcomes to our clients, investors, shareholders, counterparties, employees, markets, competition, and provide all colleagues with a fair and safe working environment that is free from discrimination, exploitation, bullying, harassment, or inappropriate language. As Conduct Risk may arise from anywhere in the Group and across all **Principal Risk Types** (PRTs) at any given moment, the Group expects all employees to be

¹ SC Ventures (SCV) is the business unit within the Group that promotes innovation, invests in disruptive technologies, and explores alternative business models.


responsible for managing Conduct Risk. RFOs must assess the impact of the conduct outcomes identified and managed through the respective PRTs.



- 3.3 The global business **Chief Executive Officers** (CEOs), product heads, functions heads, as well as cluster and country CEOs are responsible for ensuring that employees identify, mitigate, and monitor Conduct Risk.
- 3.4 The Group Head, **Conduct, Financial Crime and Compliance** (CFCC) is responsible for setting standards which include expectations of the First and Second **Lines of Defence** (LoD) and for providing adequate oversight and challenge of Conduct Risk management across the Group. The Group Head, CFCC delegates responsibility for Conduct Risk Management to the Global Head of Frameworks and Policies.
- 3.5 The Group must demonstrate that Conduct Risk is always considered when making material strategic decisions that may impact clients, investors, shareholders, counterparties, employees, markets, competition, and the environment. The Audit Committee provides board-level oversight over Conduct Risk management.
- 3.6 A view on the overall impact on conduct outcomes will be considered by the Group Head, CFCC in the annual review of Conduct Risk Management approach.

4. Three Lines of Defence

- 4.1 The Group applies a three LoD model to its day-to-day activities for effective risk management, risk governance and the control environment. Typically:
 - The businesses and functions engaged in or supporting revenue generating activities that own and manage the risks constitute the **First Line** (1LoD).
 - The control functions independent of the 1LoD that provide oversight and challenge of risk management, to offer confidence to the GCRO, Senior/Executive Management and the Board, act as **Second Line** (2LoD).
 - Internal Audit as the **Third Line** (3LoD) provides independent assurance on the effectiveness of controls supporting the activities of the 1LoD and 2LoD.
- 4.2 Key responsibilities across the three LoD are summarised in Table 1 below:

Table 1: Three Lines of Defence

LoD	Key responsibilities
First (1LoD) 	<ul style="list-style-type: none"> ▪ Promote a healthy risk culture and good conduct. ▪ Propose the risks required to undertake the revenue generating activities. ▪ Own and design processes, controls, and procedures for complying with the risk management frameworks, policies, and standards. ▪ Identify, assess, mitigate, monitor, and escalate risks and issues to 2LoD and to Senior Management Functions (i.e., individuals designated under the Financial Conduct Authority (FCA) and PRA Senior Managers Regime (SMR)). ▪ Manage risks within approved Group Board RA. ▪ Set and execute remediation plans where a risk has materialised. ▪ Validate and self-assess compliance with frameworks and relevant policies, confirm the quality of validation, and provide evidence-based affirmation to 2LoD. ▪ Ensure systems and processes meet risk reporting, risk data aggregation and data quality requirements set by the 2LoD. ▪ Ensure that applicable laws and regulations are complied with through implementation of appropriate end-to-end processes and controls, and escalate significant regulatory non-compliance matters to the 2LoD and Senior/Executive Management. ▪ Manage risk to protect business services from disruption to the extent practicable. ▪ Identify all support required for Important Business Services, and ensure the operations are within Impact Tolerances, including under severe but plausible scenario disruptions

LoD	Key responsibilities
Second (2LoD) 	<ul style="list-style-type: none"> Promote a healthy risk culture and good conduct. Review 1LoD risk proposals and make decisions as appropriate. Oversee and challenge 1LoD risk taking activities. Develop frameworks, policies, and standards, for the mitigation of risk for the PRT and monitor compliance. Own and manage processes for oversight and challenge. Propose RA metrics to the Board and monitor and report on adherence to those metrics. Propose Management Team Limits and monitor and report on adherence to these limits. Intervene to curtail business if it is not in line with existing or adjusted RA, if there is material non-compliance with policy requirements or operational controls do not effectively manage risk. Ensure effective implementation of the frameworks and relevant policies and affirm the effectiveness to RFO or the GCRO (see section on <u>Policy Owner responsibilities</u>). Identify, assess, mitigate, monitor, and escalate risks and issues to the GCRO, Group and country Senior/Executive Management and the Group and country Board or Board-level committees. Review and challenge risk remediation plans set by the 1LoD to mitigate RA breaches or issues. Set risk reporting, risk data aggregation and data quality requirements and ensure that systems and processes meet these requirements. Ensure that there are appropriate controls and requirements in place to comply with applicable laws and regulations and escalate significant regulatory non-compliance matters and developments to the GCRO, Group and country Senior/Executive Management and the Group and country Board or Board-level committees.
Third (3LoD) 	<ul style="list-style-type: none"> Help the Board and Senior/Executive Management protect the assets, reputation, and sustainability of the Group. Assess if all key risks have been identified and reported to the Board and Senior/Executive Management in line with the established risk management processes. Independently assess the adequacy and effectiveness of risk management, controls, and governance framework processes.

- 4.3 In cases where Functions act as both 2LoD for oversight and challenge and 1LoD for their own operational activities, it is mandated that the operational units and 2LoD units are segregated to fulfil the independence requirement of the 2LoD. In addition, these 1LoD activities are subject to oversight and challenge as part of the **Risk and Control Self-Assessment (RCSA)** and Response Management approach by the appropriate oversight function².
- 4.4 The detailed set of global and country-level roles and responsibilities for the 1LoD and 2LoD, including any adaptations of the above-mentioned principles to the specifics of each PRT, are provided in the respective frameworks in Part B.

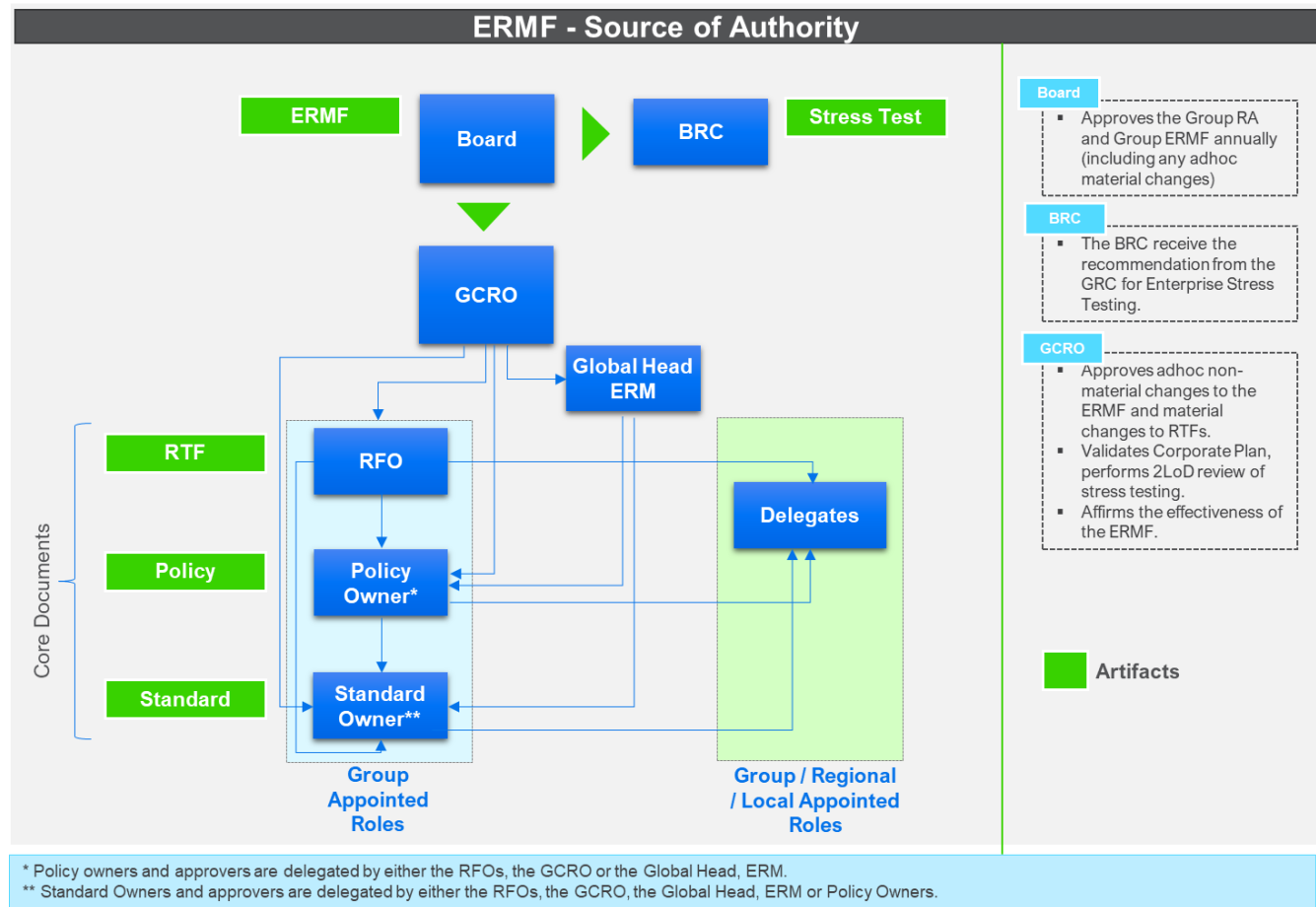
5. Source of Authorities

- 5.1 Individuals may receive their authority from the Board, committee resolutions, this Framework (including the RTFs), Policies, the **Group Delegated Authorities Manual (GDAM)**, Group Authorities Signature Book and Powers of Attorney.
- 5.2 Individuals may also receive authority through designated **Senior Management Functions (SMFs)** and Certified Person appointments. Furthermore, individuals may receive authority from their job descriptions and delegation of authority letters.
- 5.3 All risk authorities required to implement this Framework and manage the PRTs are delegated by the Board to the GCRO.

² This oversight function would typically be OTCR, CFCC, Model or ESGR depending on the risk and subject matter expertise.

5.4 Through this Framework, the GCRO appoints the RFOs for the management of the PRTs and delegates authorities required to discharge their responsibilities. See Figure 1 below.

Figure 1: Source of Authority



5.5 The RFOs may delegate authorities to designated individuals through the respective RTFs³, including 2LoD ownership at global business, product, and functional level as well as country level.

6. Committees and Meetings

6.1 The corporate governance and committee structure helps the Group to conduct our business to the highest standard of governance. Different types of governance meetings exist within the Group, characterised by distinct levels of formality and operational requirements.

6.2 Committees are *formal governance bodies appointed by a higher authority (for example, in the case of Board Committees, the Board), with the power to consider, review, recommend and make decisions that are separate and distinct from the authority of its individual members*⁴.

6.3 Other types of governance meetings may also be established, with the primary purpose to aid communication, alignment, engagement and / or drive performance delivery. These meetings are characterised by a lower level of formality and operational requirements compared to committees.

6.4 The scope of committees and other governance meetings can be group-wide or entity-level specific.

Executive and Board level Committees

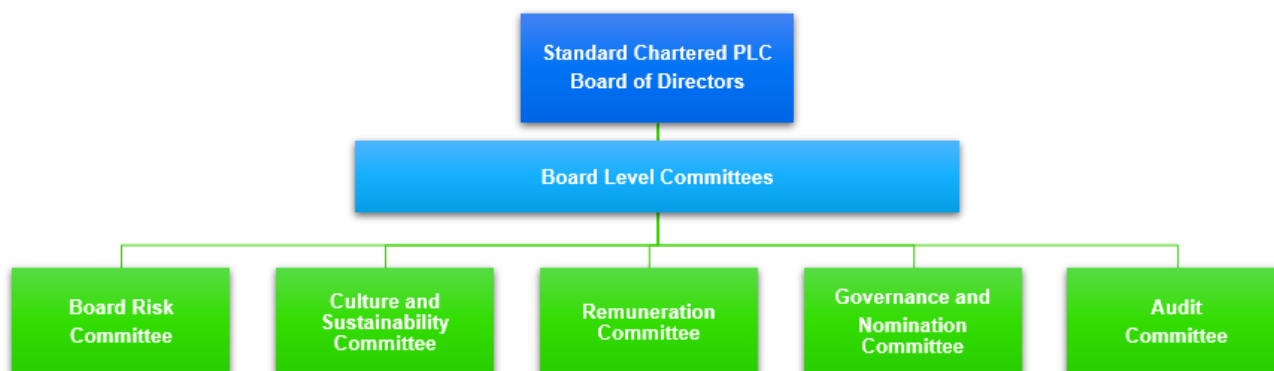
6.5 The committees described in this section derive their authority from the Board, the Group CEO, Group CFO and Group CRO.

³ RFOs must ensure that RTFs are supported by the required Policies and Standards. The RFOs are the document approvers for these Policies and Standards but may delegate this responsibility. These delegations are outlined in ERMF Part C2 and C5.

⁴ The scope of a Committee's responsibilities and the identity of its appointing authority are contained within its terms of reference which also set out the Committee's purpose, membership, quorum and operations.

- 6.6 The Board has ultimate responsibility for risk management and is supported by the five Board-level committees. The Board approves this Framework based on the recommendation of the **Board Risk Committee** (BRC) which also recommends the Group RA for all PRTs and other risks. See Figure 2 below.

Figure 2: Board-level committee structure



- 6.7 In addition to the BRC and the **Audit Committee** (AC), the **Culture and Sustainability Committee** (CSC) oversees the Group's culture and key sustainability priorities.
- 6.8 Senior/Executive Management must ensure that the Board is provided with the necessary information to exercise its oversight function.
- 6.9 Senior/Executive Management must provide the Board with full yet appropriately calibrated information. They must disclose and escalate clearly anything that the Board would be reasonably expected to take notice of.
- 6.10 Senior/Executive Management should periodically ensure that the type, frequency, and volume of information it provides to the Board meets the Board's oversight function.
- 6.11 The **Group Risk Committee** (GRC), which derives authority from the GCRO, ensures effective management of risk throughout the Group in support of the Group's strategy. The GRC oversees effective implementation of this Framework for the Group.
- 6.12 The GCRO, as Chair of the GRC, approves the use of sub-committees to support the GRC in overseeing risk at various levels of the organisation as appropriate. The **Global Head, Enterprise Risk Management** (Global Head, ERM) sets **Committee Governance Standards** (CGS) for the GRC and its sub-committees. The appointed chairpersons of these committees must perform committee effectiveness reviews at least annually. The **Terms of Reference** (ToR) for the GRC and its one-down committees can be found [here](#).
- 6.13 The **Group Asset and Liability Committee** (GALCO), appointed and chaired by the **Group Chief Financial Officer** (GCFO) is responsible for providing oversight on Treasury Risk by determining the Group's approach to balance sheet strategy, recovery planning and ensuring that, in executing the Group's strategy, the Group operates within approved RA.
- 6.14 Risk committees are responsible for determining their own risk reporting requirements and ensuring that they receive all relevant information required to fulfil their governance mandate.

7. Principal Risk Types

- 7.1 PRTs are those risks that are inherent in our strategy and business model. They are managed through distinct frameworks that document the overall risk management approach for the respective PRT.
- 7.2 As part of the annual review of this Framework, the Global Head, ERM reviews the list of PRTs and proposes any necessary changes as required to the GCRO. The proposed changes to PRTs should consider the Group's **Risk Identification** (Risk ID) process as outlined in Section 11, and recommendations from the risk impact analysis of the Corporate Plan. The list of PRTs is approved by the Board.

- 7.3 The GCRO appoints the RFOs for 2LoD oversight and challenge for each of the PRTs⁵. Please refer to Table 2 below for the list of PRTs and RFOs.

Table 2: PRTs and RFOs

PRT	Definition	RFO
Credit	Potential for loss due to failure of a counterparty to meet its agreed obligations to pay the Group.	Co - CRO, Corporate and Investment Banking (CIB) & ASEAN & South Asia CRO, Wealth & Retail Banking (WRB) & GCNA
Traded	Potential for loss resulting from activities undertaken by the Group in financial markets.	Global Head, Traded Risk Management
Treasury	Potential for insufficient capital, liquidity, or funding to support our operations, the risk of reductions in earnings or value from movements in interest rates impacting banking book items and the potential for losses from a shortfall in the Group's pension plans.	Global Head, ERM
Operational and Technology	Potential for loss resulting from inadequate or failed internal processes, technology events, human error, or from the impact of external events (including legal risks).	Global Head, Operational, Technology & Cyber Risk
Financial Crime	Potential for legal or regulatory penalties, material financial loss or reputational damage resulting from the failure to comply with applicable laws and regulations relating to international sanctions, anti-money laundering and anti-bribery & corruption, and fraud.	Group Head, Conduct, Financial Crime, Compliance
Compliance	Potential for penalties or loss to the Group or for an adverse impact to our clients, stakeholders or to the integrity of the markets we operate in through a failure on our part to comply with laws, or regulations.	Group Head, Conduct, Financial Crime, Compliance
Information and Cyber Security	Risk to the Group's assets, operations, and individuals due to the potential for unauthorised access, use, disclosure, disruption, modification, or destruction of information assets and / or information systems.	Global Head, Operational, Technology & Cyber Risk
Environmental, Social and Governance and Reputational (ESGR)	Potential or actual adverse impact on the environment and/or society, the Group's financial performance, operations, or the Group's name, brand or standing, arising from environmental, social or governance factors, or as a result of the Group's actual or perceived actions or inactions.	Global Head, ERM
Model	Potential loss that may occur because of decisions or the risk of mis-estimation that could be principally based on the output of models, due to errors in the development, implementation, or use of such models.	Global Head, ERM

8. Roles and Responsibilities - Control Model

8.1 Purpose of the Control Model

- 8.1.1 The purpose of the control model is to outline the three-tier control documents hierarchy, the associated roles, and the overall governance.

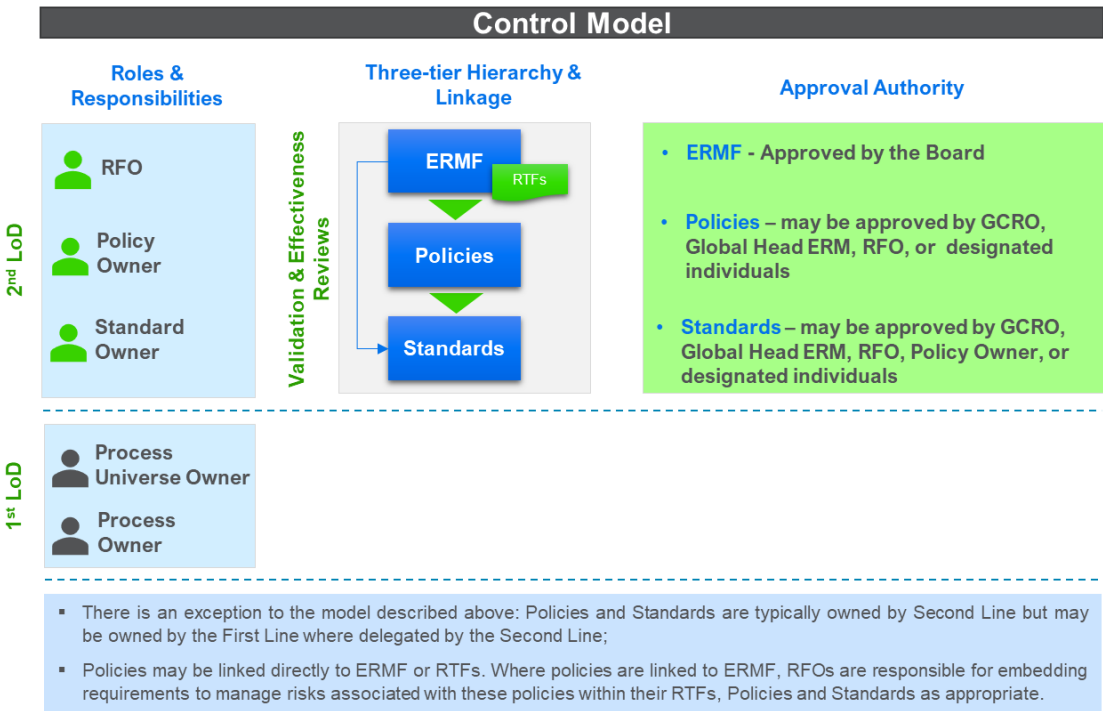
⁵ In line with the Senior Management Function and Statement of Responsibilities (SoR), Group Head, CFCC has direct oversight of the Compliance and Financial Crime PRTs.

- 8.1.2 The Group must comply with all applicable laws and regulations⁶. The Group refers to **Group-wide Regulations** to mean the regulatory baseline to be applied across the Group. It comprises:
- Obligations which arise from laws and regulations issued by Group regulatory authorities based in the UK (e.g., PRA, FCA) and international standards setters or policy setters (e.g., Basel Committee, IOSCO, FSB, etc.).
 - Obligations which arise from local/country regulators (e.g., HKMA, MAS, RBI) if they are extra-territorial (i.e., applicable beyond the territorial boundary of the issuing regulator)
 - Supranational authorities (e.g., EU, OECD), which may issue extra-territorial regulatory obligations, and therefore, these may be managed at Group level.
- 8.1.3 The exact baseline is defined by Group RFOs, Policy Owners and Standard Owners in their 2LoD capacity.
- 8.1.4 In addition to externally imposed obligations the Group may voluntarily choose to adopt certain business practices or make specific commitments to its stakeholders.

8.2 Overview of the Control Model

- 8.2.1 The Control Model promotes compliance with applicable laws and regulations, as well as voluntarily chosen business practices and commitments by the Group.
- 8.2.2 The model provides clear lines of authority and responsibilities and is documented through a structured document hierarchy which comprises frameworks, policies, standards.
- 8.2.3 The following roles are formalised for effective implementation of this Framework:
- Risk Framework Owner
 - Policy Owner
 - Standard Owner
 - Process Universe Owner
 - Process Owner
- 8.2.4 The Global Head, ERM sets governance standards for these in the *Framework and Policy Governance Standard* (FPGS). See Figure 3 below.

Figure 3: Control Model



⁶ These regulations include those from Financial Services Regulatory Authorities and other regulators that may issue regulations pertaining to the Group (e.g., Health & Safety regulation). Regulations may be issued in forms that include but are not limited to guidelines and notices.

8.3 Control Model Documents

- 8.3.1 To address externally imposed obligations, the control documents hierarchy comprises Frameworks, Policies, and Standards which, alongside the obligations register (or equivalent forms of maintaining a full list of the obligations), must provide a clear and comprehensive view of all the applicable obligations and facilitate full traceability of the requirements.

Definition and Principles for the RTFs

- 8.3.2 RTFs are “*developed for all PRTs outlining the governance and risk management approach specific to the PRT*”. These must cover the following at minimum:
- Key roles and responsibilities across 1LoD and 2LoD
 - Decision making authorities and delegation of authorities
 - Group and local level committees.

Additional details on the core elements of the RTFs are set out in Chapter 1 of Part B.

Definition and Principles for Policies

- 8.3.3 Policies are “*a set of internal rules and principles that are established to help the Group to adhere to external or internal requirements. Policies guide decision-making, process design and desired behaviour in the Group⁷ through policy statements*”.
- External requirements are prudential⁸ and non-prudential rules and expectations from a range of rule setters (mainly regulators, supervisory authorities, and legislators).
 - Internal requirements are business requirements that management voluntarily chooses to introduce to pursue Group objectives; for instance, by adopting best practices or meeting voluntary commitments to our stakeholders⁹.
- 8.3.4 Policy documents must articulate why the policy objectives are important; and set expected practices to meet those objectives.
- 8.3.5 Procedural information that details how to achieve the policy objectives should not feature in policies; these should be covered in Standards or **Department Operating Instructions (DOI)**.
- 8.3.6 Policies may be linked to RTFs or directly to the ERMF. Where policies are linked to ERMF (i.e., outside of a specific RTF), these need to outline the following at minimum:
- Risk management principles.
 - Key roles and responsibilities covering 1LoD and 2LoD.
 - Decision making authorities and delegation of authorities.
 - Governance framework.
 - Approach to RA, risk assessment, risk reporting, risk data aggregation and data quality.
 - Approach for local-level implementation for branches and / or banking subsidiaries.

Definition and Principles for Standards

- 8.3.7 Standards are “*companion documents to framework and policies. They are tools for the Policy Owner to translate policy requirements into clear control objectives, and to help the Process Owners interpret the policy statements*”.
- 8.3.8 The Standards outline the minimum requirements needed to fulfil policy and RTFs objectives; thus, they are more detailed than policies.

⁷ Risk Management and Compliance are the two most common types of Policies across the Group

⁸ Prudential risks are those that can reduce the adequacy of the Group financial resources. Some key prudential risks are credit, market, liquidity, operational, insurance and group risk (FCA Handbook, PRU 1.4.3).

⁹ Our sector position statements are an example of this.

- 8.3.9 In cases where additional artefacts (e.g., DOI, process notes, obligations register or equivalent) are used to elaborate on the applicable requirements, the Standard Owner must ensure these are explicitly referenced and indexed in the Standard.
- 8.3.10 Standards are typically owned by 2LoD but may be owned by the 1LoD, where delegated by the 2LoD.
- 8.3.11 Standards must be approved by RFOs, or Policy Owners, or designated individuals identified in this Framework, or the Policy. In case of inconsistencies between Policy and underlying Standards, Policy statements will prevail.
- 8.3.12 The GCRO or Global Head, ERM can direct additional frameworks, policies, or standards as necessary to maintain the effectiveness of this Framework and appoint owners.

8.4 RFOs responsibilities

- 8.4.1 To discharge their duties with respect to Section 5.4, Part A.
- 8.4.2 RFOs are responsible for:
- Setting and maintaining the RTFs for their PRTs.
 - Ensuring that RTFs are supported by the required Policies and Standards. The RFOs are the document approvers for these Policies / Standards but may delegate this responsibility as appropriate.
 - Delegating risk authorities to designated individuals for the management of their PRT which may include the responsibility for writing, maintaining and approving policies / standards (see [Policy Owner Responsibilities Section](#)).
 - Embedding requirements to manage risks associated with policies linked directly to the ERMF¹⁰ within their RTFs, Policies and Standards as appropriate.
 - Ensuring compliance with the minimum requirements defined by the respective Policy Owners for these areas of risk.
 - Assessing the effectiveness of the RTF and quality of its implementation, in line with the provisions included in the [Effectiveness Review Standard](#).
 - Escalating significant risks and issues to the GCRO, the Senior/Executive Management and the Board or Board-level committees.
 - Providing an annual affirmation to the GCRO on the effective management of the PRT. The affirmation must be evidence-based and will be subject to review and challenge by the Global Head, ERM.
 - Providing an affirmation to the relevant Senior Manager Function to confirm that the respective RTF and related Policies and Standards are aligned to applicable Group-wide regulatory requirements.
 - Providing review and sign-off of regulatory attestations to confirm compliance to relevant regulations in line with the [Effectiveness Review Standard](#) and the [Group Communication with Regulators Standards](#) and maintain records of such attestation.
- 8.4.3 For local RFOs' responsibilities please refer to Section 16 (Part A) of this Framework and the [Entity Risk Governance Standard](#) (ERGS).

8.5 Policy Owner Responsibilities¹¹

- 8.5.1 Policy Owners receive a delegation from either the RFOs, the GCRO or the Global Head, ERM to write policies over specific areas of business (see section on [Source of Authorities](#) for further details). The latter must however remain accountable and oversee the Policy Owner's activities.
- 8.5.2 Policy Owners must ensure:
- The policy is fit for purpose in terms of scope and content - To be fit for purpose, policies must be kept up to date to reflect the latest Group-wide regulations (see [Managing Group-wide Regulatory](#)

¹⁰ Some examples include, Risk Appetite Policy, Climate Risk Policy, Digital Assets Risk management Policy

¹¹ For the **Treasury Risk**, the Policy / Standard Owner responsibilities described in this section 8.5 Part A (paragraphs I. to V.) follow a different allocation between First Line (Group Treasurer) and Second Line (Treasury CRO and Treasury Risk RFO). See Treasury Risk Type Framework within Part B for details.

Obligations section 8.5.3.I). Secondly, they must outline internal roles and responsibilities for implementation. Finally, they must be presented in a logical and concise manner.

- Policies under their ownership are managed effectively through the policy lifecycle – Policy Owners are responsible for end-to-end lifecycle of policies, which starts from drafting and consultation through to communications and training.
- Establish a mechanism to assess the quality of implementation – The Policy Owners must provide oversight and challenge to the parties that implement the Policies and affirm internally or externally, if needed, the effectiveness of the Policy.

8.5.3 The Policy Owners responsibilities are outlined below:

I. **Managing Group-wide regulatory obligations**

Responsibilities include:

- a) Maintain a full list of regulatory authorities anywhere in the Group's footprint which may issue regulations with Group-wide impact and define applicable types of publication for horizon scanning¹².
- b) Interpret regulations which are in force or expected to come into force. This includes performing an impact assessment and gap analysis to cover new regulations vs. current Policy / Standards requirements.
- c) Establish a mechanism to assess Group-wide regulations and ensure that all requirements are covered within policies and / or standards. This includes:
 - Identify and document at a high level in the Policy all applicable Group-wide Regulations within their area of responsibility and the scope of the Policy.
 - Ensure complete and accurate traceability, where applicable by way of the obligations register or equivalent, to demonstrate that Policy statements and / or Standards have been mapped upstream to the source of the obligation by Policy Owner and downstream to controls identified by Process Owner¹³.
 - Ensure that requirements are communicated to 1LoD or relevant Process Owner for implementation.

II. **Defining requirements for documenting end-to-end processes and key controls**

Whilst the Process Owner is mandated to document end-to-end processes in line with the Process Owner responsibilities section, Policy Owners must:

- a) Outline in the Policy and / or Standards key processes and / or systems subject to the control requirements.
- b) Ensure Standards outline all minimum requirements to fulfil Policy intentions and translate these into clear control objectives.

III. **Drafting and Communicating Policies**

Policy Owners are responsible for drafting, maintaining, and communicating Policies and for ensuring training is delivered, as relevant, to support their implementation. The FPGS standard outlines the detailed requirements for the governance of policies.

Policy Owners must ensure that the Policies:

- a) Define their geographic, business, or functional scope.
- b) Clearly articulate the objectives of the Policy, for example the critical risks or critical processes it is designed to address.

¹² The Regulation Identification Unit ("RIU") is a Risk and Compliance utility team which may be delegated by a Policy / Standard Owner to perform this step and disseminate the rules to the owners.

¹³ Provisions in paragraph 8.5.3(I).c) with reference to mapping "downstream to controls identified by the process owner" are not immediately applicable. Work is underway to establish an effective date for this plan. More time is required to assess complex interdependencies, including FFG initiatives.

- c) Define the mandatory Policy statements with actionable principle-based requirements that can be reasonably validated and / or evaluated for effectiveness.
- d) Clearly outline the roles and / or job families responsible to comply with Policy requirements.
- e) Identify the Standards underlying the Policy, ensuring their consistency with the Policy.
- f) Clearly set out policy specific authorities and decision-making matrix, including dispensations, and escalations requirements.
- g) Identify key areas of connectedness and cross reference to other governance documents.
- h) Set all necessary requirements for risk reporting, risk data aggregation and data quality.

IV. Affirmation on Policy Effectiveness

The Policy Owner must provide an annual affirmation to the relevant RFOs or GCRO on Policy effectiveness. The affirmation must be substantiated with evidence.

At a minimum, the affirmation must consider the effectiveness of key controls and highlight the impact that known control deficiencies may have on the ability of the Group to maintain compliance with laws and regulations¹⁴.

V. Oversight of the end-to-end process for managing Policies

The Policy Owner is responsible to maintain oversight of the end-to-end process including:

- a) Ensuring effective implementation of the Policies (and related Standards) and affirming its effectiveness to RFOs or the GCRO.
- b) Escalating significant risks and issues to relevant RFOs, GCRO, Senior/Executive Management, the Board or Board-level committees, including, but not limited to, any regulatory non-compliance matters and developments.
- c) Review and challenge of risk remediation plans set by the 1LoD to mitigate RA breaches or issues relevant to the policy.
- d) Intervening to curtail business where material non-compliance with Policy requirements is reported or when operational controls do not effectively manage inherent risks.

Policy Owner may delegate responsibility for duties listed above from point I) to V) to Standard Owners. In this instance:

- the Policy Owner remains accountable for all expected outcomes.
- the Policy Owner must maintain oversight of the Standard Owners' activities¹⁵ irrespective of whether the Standard Owner is in the 1LoD or 2LoD.

8.5.4 For the handling of local regulatory obligations¹⁶, please refer to Section 16 (Part A) of this Framework and the [ERGS](#) which define the requirements for local RFOs to follow in this respect.

8.6 Standard Owner Responsibilities

8.6.1 A Standard Owner receive delegation from either the RFOs, the GCRO, the Global Head, ERM or Policy Owners. Based on this delegation and considering the different scope and purpose of Standards¹⁷ compared to policies, the Standard Owner's responsibilities are the same as a Policy Owner and follow those outlined above in section 8.5 above (section I. - V.).

¹⁴ For details of how to perform the internal affirmation, please see the [Effectiveness Review Standard](#).

¹⁵ For details of how the Policy Owners' oversight responsibilities over the Standard Owners' activities may be discharged, please see the [Effectiveness Review Standard](#).

¹⁶ Regulatory obligations to be implemented at local level which may emanate from both extra-territorial regulations and local regulatory authorities.

¹⁷ See section 8.3 for definition and purpose of Standards.

8.7 Process Universe Owner and Process Owner Responsibilities

- 8.7.1 Process Universe Owners are Global Heads (Businesses CEOs, Global Product Heads and Global Function Heads) and are responsible to take reasonable steps for:
- Identifying processes within their respective business or function, and completeness and accuracy of such identified processes.
 - Ensuring that all the processes have named Process Owners and are in compliance with the Operational Risk Standards and the RCSA requirements.
 - Reviewing, challenging, and providing oversight of the risk profile and the RCSA through the Non-Financial or other Risk Committees.
 - The local / Country CEOs are responsible for overseeing the execution of local / country-level processes in line with standards set by the Global Process Owners and Policy Owners and monitor local deviations to global Standards.
- 8.7.2 Process Owners are business or function managers responsible for the end-to-end business or function processes as identified within the Group's Process Universe. They are responsible for:
- I. **Documenting end-to-end processes:**
 - Identification, management, and documenting of the end-to-end process as defined in the Group's Process Universe, including activities which are carried out by other businesses or functions, or which are under a hub arrangement or outsourced.
 - This includes consideration of the applicable regulatory requirements and the agreed implementation as mandated in relevant Policy and Standards.
 - Ensuring independence is maintained in the end-to-end process to avoid any potential areas of conflict, including oversight activities (refer to 4.3).
 - II. **Identifying key risks and implementing key controls:**
 - Identifying the risks associated with these end-to-end processes and **designing key controls for implementation**, in line with the provisions included in relevant Policies and Standards.
 - Being responsible to the Process Universe Owner, RFOs and / or Policy Owners
 - **Implementing the controls to comply with the requirements** set out in the relevant Policies / Standards.
 - III. **Monitoring and testing of controls' effectiveness:**
 - Implementing through the RCSA a common and systemic approach to monitor the effectiveness of the controls and standards governing the end-to-end process as outlined in the Group Operational Risk Policy and Standard.
 - Maintaining complete records of all risk events and performing impact assessment and review of Risk and Controls outcomes.
 - IV. **Attesting to RFOs and / or Policy Owners on effectiveness of controls**
 - Process Owners in both, the 1LoD and 2LoD must validate and self-assess compliance to the control requirements, confirm the quality of validation, and provide evidence based self-assessments to the RFOs and Policy Owners on the adequacy and effectiveness of performance of their processes to the prescribed control requirements.
 - This attestation must include, at minimum, a self-assessment on controls implemented to ensure compliance with applicable laws and regulations and escalation of any significant regulatory non-compliance matters and developments to the Process Universe Owner, Policy Owner, and Senior/Executive Management (refer to 8.5.3 (I)c, bullet 2)
 - 2LoD process owners should coordinate with an independent unit for oversight and challenge of requirements set by their own frameworks or policies to avoid potential conflict of interest (refer also to section 4.3).
 - V. **Reporting and escalation:**
 - Escalating significant risks and issues to the Process Universe Owners, relevant RFOs and/or Policy Owners.

- 8.7.3 Process Owners and their teams may develop DOIs, process and / or guidance notes. These optional documents may be used to implement policies and standards but also for other purposes, including for organising departmental workflows, delineating the scope of team activities, and managing a portfolio of work. The document owner shall ensure that:
- these documents are maintained up to date and, where applicable, consistent with the relevant policies and standards; and
 - are cascaded to all relevant parties and remain easily accessible for execution.

These documents are not part of the Control Model hierarchy. In case of any inconsistency, reference must be made to the policies and standards for final authority.

9. Group Strategy and Strategic Risk Management

- 9.1 The Board is responsible for approving that the Group Strategy and five-year Corporate Plan is in line with the approved Board **Risk Appetite** (RA).
- 9.2 The Group Chief Executive, the **GCRO** and the **GCFO** are responsible for ensuring that the Group strategy and Corporate Plan align with this Framework and the Board RA.
- 9.3 The GCRO delegates the review of critical risk management components within the Corporate Plan to the Global Head, ERM. Please refer to Figure 4 below:

Figure 4: Group Strategy and Strategic Risk Management



- **Group Strategy and Risk Identification:** As part of the Group Strategy review process, the business CEOs are responsible to prepare an impact analysis of risks that arise from the growth plans, strategic initiatives, and the business model vulnerabilities. This impact analysis should identify whether existing risks have changed in terms of relative importance or new risks have been introduced. The Global Head, ERM reviews and prioritises existing and/ or new risks, and recommends to the GCRO for consideration in the annual review of this Framework.
- **Group Strategy and RA:** As part of the Group Strategy review process, the business CEOs are responsible to prepare an impact analysis to confirm that the growth plans and strategic initiatives are within approved RA and highlight areas where additional RA should be considered. The Global Head, ERM reviews the alignment between Group Strategy and the Group RA and will escalate areas of misalignment to the GCRO.

- On behalf of the GCRO, the Global Head, ERM should review and challenge the Corporate Plan based on the risks highlighted in the plan, cross referencing against existing risks identified through the Group's various risk identification process, assessing alignment to RA, and analysing the stress test results. The GCRO can recommend adjustments for the Board's consideration at the time of review and approval of the Corporate Plan.
- **Group strategy and stress testing:** Outcomes from the risk highlighted during this process and other risk identification processes are used to develop scenarios for enterprise stress tests. In order to ensure that the Group Strategy remains within the Board-approved RA, the GCRO and GCFO can recommend strategic actions based on the stress test results. Stress test results must be considered in the setting of the Group RA (refer to section 10 below).

9.4 The business CEOs are responsible for performing periodic assessments of the implementation of the Group strategy for their businesses, and escalate matters to the Group Chief Executive, GCFO and GCRO through Group performance reviews. Significant matters should also be highlighted to Global Head, Strategy, Group Head, Finance, and Global Head, ERM for consideration in the risk identification activities conducted across the Group.

10. Group Risk Appetite Framework

- 10.1 The Board is responsible for approving the Group Risk Appetite (RA), based on the recommendation of the GCRO, and the BRC. The GCRO delegates to the Global Head, ERM the process to maintain, set, monitor and remediate RA, and assess the Corporate Plan against RA. The RA should be periodically reviewed by the Board at the end of year along with the Corporate Plan, with an interim review if necessary. A review can also be triggered by material change in circumstances arising from the internal or external environment.
- 10.2 The Group RA is defined as *"the approved boundary for the risk that the Group is willing to undertake to achieve the Group strategic objectives and Corporate Plan"*. It is set within the Risk Capacity which is defined as *"the maximum level of risk the Group can assume, given its current capabilities and resources, before breaching constraints determined by capital and liquidity requirements, internal operational environment, or otherwise failing to meet the expectations of regulator and law enforcement agencies."*
- 10.3 The Group RA includes:
- Group **Risk Appetite Statements** (RAS) for the PRTs, based on materiality and significance for Board level attention.
 - RA metrics and thresholds for strategic areas.
- 10.4 A breach of Group RA occurs when the Group's measured performance is outside of RA threshold for a Board approved RA metric.
- 10.5 In addition, **Management Team limits** (MTL) are established to support the management and monitoring of the RA metrics. The GRC decides which MTLs to use and approves the MTL metrics thresholds. Breaches of both RA and MTL metrics are reported to the BRC / GRC / GALCO with required remediation plans, in line with the Risk Appetite Policy and Standards. In addition to the PRTs', RAS, RA and MTL metrics may also be defined for other areas of risk, where applicable.
- 10.6 The RAS for the Group is set out in Table 3 below:

Table 3: Group Risk Appetite Statements

	Description
General	The Group will not compromise adherence to its Risk Appetite in order to pursue revenue growth or higher returns.
Credit Risk	The Group manages its credit exposures following the principle of diversification across products, geographies, client segments and industry sectors.
Traded Risk	The Group should control its financial markets activities to ensure that market and counterparty credit risk losses do not cause material damage to the Group's franchise.

	Description
Treasury Risk	The Group should maintain sufficient capital, liquidity and funding to support its operations, and an interest rate profile ensuring that the reductions in earnings or value from movements in interest rates impacting banking book items does not cause material damage to the Group's franchise. In addition, the Group should ensure its Pension plans are adequately funded.
Operational and Technology Risk	The Group aims to control operational and technology risks to ensure that operational losses (financial or reputational), including any related to conduct of business matters, do not cause material damage to the Group's franchise.
Information and Cyber Security Risk	The Group aims to mitigate and control ICS risks to ensure that incidents do not cause the Bank material harm, business disruption, financial loss or reputational damage – recognising that whilst incidents are unwanted, they cannot be entirely avoided.
Financial Crime Risk*	The Group has no appetite for breaches in laws and regulations related to Financial Crime, recognising that whilst incidents are unwanted, they cannot be entirely avoided.
Compliance Risk	The Group has no appetite for breaches in laws and regulations related to regulatory non-compliance; recognizing that whilst incidents are unwanted, they cannot be entirely avoided.
Environmental, Social and Governance and Reputational (ESGR)	The Group aims to measure and manage financial and non-financial risks arising from climate change, reduce emissions in line with our Net Zero strategy and protect the Group from material reputational damage by upholding responsible conduct and striving to do no significant environmental and social harm.
Model Risk	The Group has no appetite for material adverse implications arising from misuse of models or errors in the development or implementation of models; whilst accepting some model uncertainty.

* Fraud forms part of the Financial Crime RAS but in line with market practice does not apply a zero-tolerance approach

- 10.7 As part of the RA reviews, the RFOs must assess RA metrics and thresholds for their respective PRTs, and propose necessary revisions to the Global Head, ERM for consideration. The RA metrics must consider inherent risks associated with the PRT and their sub-types, control effectiveness and residual risk or outcome-based metrics. Where applicable, RA metrics must be forward looking and consider downside volatility by calibrating thresholds under stress scenarios. The Global Head, ERM should collectively assess the RA metrics and thresholds across all PRTs and make recommendations to the GCRO.
- 10.8 RA metrics and thresholds follow the approval authorities set out in the [Risk Appetite Policy](#) and the [Group Risk Appetite Standard](#).
- 10.9 The GCRO takes the Group RA to the BRC to obtain its support for subsequent Board approval. Prior to approval of the Corporate Plan, the GCRO must validate that it is consistent with the Group RA.
- 10.10 For changes outside of the Annual and Interim Risk Appetite review cycle, the Board delegates authorities to the GCRO as outlined in table 4. The GCRO can approve increases in MTL of up to ten percent without prior notification to the GRC. The GRC delegates authorities to relevant RFOs in relation to any decrease in approved MTL. All out of cycle changes must be notified to the next GRC. Risk Appetite changes must also be notified to the next BRC. Approvals are valid until the next interim or annual review.

Table 4: Out of Cycle Approval Authority for Risk Appetite

Metric threshold change	Amount	Delegating Body	Delegated Approval Authority
Increase	An increase of up to ten percent of the approved limit	SC PLC Board	GCRO, with prompt notification to the BRC Chair and the Group Chief Executive
Decrease	Any decrease in the approved limit	SC PLC Board	GCRO, with prompt notification to the BRC Chair and the Group Chief Executive

- 10.11 To ensure that RA is adhered to, all RFOs must consider a RA allocation mechanism that suits the risk profile of their PRTs. This should be an allocation to the most relevant organisational dimensions, such as material group subsidiaries, individual businesses or branches, specific risk categories, concentrations, and where risk is expected to be managed by the 1LoD. Allocated metrics must be relevant, measurable, and controllable for the applicable business segment, product, or legal entity. The RA threshold calibration principles are:
- RA allocated to relevant organisational dimensions must not exceed the total of Group RA (at cumulative level).
 - For limits which are not perfectly additive (for example, value at risk or some portfolio limits), the allocation may consider diversification benefits.
 - RA thresholds must be calibrated based on the level of risk deemed acceptable and affordable. Where possible this should be assessed under a stress scenario.
 - Any other PRT specific principles may be defined within the respective RTFs.
- 10.12 RA is also informed by stress results, with the affordability of RA under stress assessed where possible in each exercise. Where areas of excess are identified, RA is reviewed and may be recalibrated accordingly.
- 10.13 Breaches of RA and MTL metrics must be remediated in line with the requirements set out in the Group Risk Appetite Standard.
- 10.14 The principle of prompt action embedded within this Framework is supported by the Group's recovery indicators which are a set of strategic, business-related and market metrics, aligned to the ERMF. They are designed to enable a firm's management, Board, and supervisor to appropriately respond with the type and timing of the recovery options. The metrics are periodically reviewed by the Treasurer (and the Treasury CRO) in determining the **Group Stress Rating (GSR)**. An increase in the GSR would enact the Group Recovery Plan and trigger consideration of recovery options. Most of the recovery indicators are linked to the ERMF as these are based on RA. Additional market-based metrics are included to help with early alerts for a potential crisis. Recovery indicators also exist for the Group's material legal entities.
- 10.15 The GCRO, Executive and Board-level committees, and the Board review written reports to monitor compliance with the Board-approved Group RA. The GCRO can place restrictions on business activities to prevent or remediate breaches of the Group RA.

11. Enterprise Risk Identification, Assessment, Mitigation and Monitoring

- 11.1 Risk ID complements the existing Risk Appetite Framework, within which are metrics across all risk types designed to capture the full spectrum of risk drivers across the Group. These are categorised to RA metrics which depict Group-wide, strategic risks, as well as key regulatory concerns and concentrations. Below that sit the MTL metrics which are focused on functions or countries/markets. They highlight important business concerns but not a strategic focus.
- 11.2 There are multiple approaches to Risk ID that exists across the Group including RCSA, stress testing, and topical and emerging risk process, including the emerging risks survey.

- 11.3 The Global Head, ERM maintains a risk taxonomy of risks inherent to the strategy and business model; as well as a risk inventory which captures identified risks to which the Group is or might be exposed to. New risks are added as they are identified through the Corporate Plan, topical and emerging risks or other processes. The risk inventory is maintained with inputs on the internal and external risk environment, as well as potential threats and opportunities from a business and client perspective.
- 11.4 Topical risks refer to *“themes that may have emerged but are still evolving rapidly and unpredictably, whilst emerging risks refer to unpredictable and uncontrollable outcomes from certain events which may have the potential to adversely impact the Group’s business”*. This process is managed by the Global Head, ERM with input from the Risk Framework Owners, Group Strategy, Global Research, Corporate Affairs, and the Businesses.
- 11.5 The GCRO and the GRC review regular written reports on the Group’s risk profile for the PRTs, adherence to approved RA, and the Group risk inventory including the topical and emerging risks. They use this information to escalate material developments in each risk event and make recommendations to the Board on any potential changes to our Corporate Plan.
- 11.6 Each RFO must design their frameworks to ensure risks are identified, assessed, mitigated, monitored, and managed effectively.

12. Enterprise Stress Testing

- 12.1 The objective of stress testing is to support the Group in assessing that it:
- does not have a portfolio with excessive concentrations of risk that could produce unacceptably high losses under severe but plausible scenarios
 - has sufficient financial resources to withstand severe but plausible scenarios
 - has the financial flexibility to respond to extreme but plausible scenarios
 - understands the Group’s key business model risks, considers what kind of event might crystallise those risks – even if extreme with a low likelihood of occurring – and identifies, as required, actions to mitigate the likelihood and / or the impact of those events, and
 - considers how the outcome of plausible stress events may impact availability of liquidity and regulatory capital.
- 12.2 Enterprise Stress Tests are conducted at a consolidated Group-level as required by the Board, BRC, GRC, GALCO or PRA / **Bank of England (BoE)**. Legal Entity-level stress tests are also conducted at the request of local regulators.
- 12.3 Enterprise Stress Tests include:
- Capital and Liquidity Adequacy Stress Tests in the context of Capital Adequacy and Recovery and Resolution Planning.
 - Stress Tests that assess scenarios where our business model becomes challenged, such as Reverse Stress Tests.
 - Ad hoc stress tests at the BoE’s request that explore specific identified risks, such as the BoE Biennial Exploratory Scenario.
 - Climate Risk Stress Tests that assess the resilience to physical and transition risks associated with various climate related scenarios.
- 12.4 The Board delegates the approval of Enterprise Stress Tests to the BRC ahead of submission to the BoE. The BRC receive the recommendation from the GRC/GALCO.
- 12.5 The GCFO¹⁸ delegates the responsibility for Enterprise Stress Testing to the Group Head, Finance. For 2LoD oversight of stress testing, the GCFO relies on the GCRO, who delegates this responsibility to the Global Head, ERM.
- 12.6 Based on the Enterprise Stress Test results, the GCFO and GCRO can recommend strategic actions to the Board to ensure that the Group Strategy remains within the Board-approved RA.

¹⁸ The GCFO has been allocated the SMF prescribed responsibility “s” for managing the firm’s internal stress-tests, in virtue of which the responsibility for Enterprise Stress Testing is delegated to the Group Head, Finance.

- 12.7 Additionally, the Group conducts Management Stress Tests, which are internally designed and used to explore how mild plausible risks may impact the Group's ability to achieve its Corporate Plan.

13. Risk Reporting, Risk Data Aggregation and Data Quality

- 13.1 The Standard Owners of [Risk Reporting Standards](#) (RRS), [Risk Data Aggregation Standards](#) (RDAS) and [Group Data Quality Management Standards](#) (DQMS) will ensure that requirements are documented for risk reporting, risk data aggregation and data quality.
- 13.2 RFOs will ensure implementation of the risk reporting, risk data aggregation and data quality requirements in accordance with the standards mentioned above.
- 13.3 RFOs will identify priority reports and Critical Risk Measures (CRMs), which cover the minimum set of risk data required for setting risk appetite and for effective risk management in both normal and crisis situations.
- 13.4 RFOs are responsible for ensuring risk reports include exposure and position information for all significant risk areas and all significant components of those risk areas to facilitate risk management decisions.
- 13.5 RFOs will ensure that risk information allow them to identify and monitor the Group's material risks and to report to Senior/Executive Management and Board level committees. Risk reports, if applicable, will:
- provide a forward-looking assessment of risk.
 - contain forecasts and scenarios for key market variables, and relevant stress test results.
 - have the right balance of detail between qualitative and quantitative information where risk reports to senior risk committees include a greater degree of qualitative information.
- 13.6 The Group and Board risk committees should be made aware of material limitations, in terms of completeness, accuracy and timeliness of data in the risk information reports to the committees.
- 13.7 RFOs will define potential crisis situations and ensure that crisis reporting fire-drills are conducted for preparing reports in crisis situations. This includes identifying targeted enhancements to infrastructure or processes required for risk management during a crisis.
- 13.8 RFOs will define materiality considerations for infrastructure and ensure that technology infrastructure, supplemented with well-controlled manual processes, are in place to adequately support risk data aggregation and risk reporting during normal and crisis situations.
- 13.9 The Chief Transformation, Technology and Operations (TTO) Officer builds, maintains and enhances technology infrastructure to meet the risk reporting, risk data aggregation and data quality requirements defined by the RFOs. RFOs, in conjunction with TTO, will ensure that adequate resources (human and financial) are available to support required change initiatives.
- 13.10 Data quality risk can exist in sourcing, aggregation, and reporting of risk data. To ensure high quality risk data, the Board and senior management will promote the identification, assessment, and management of data quality risks.
- 13.11 RFOs and process owners (as data consumers) and Group Heads of Businesses and Functions (as data providers) should ensure that Critical Data Elements (CDEs) are defined, transformed, quality assured, documented and used appropriately in their processes. Data consumers and data providers must escalate material data quality risks to relevant committees.

14. Validation, Effectiveness Review, and Independent Assurance

- 14.1 As part of the annual review of this Framework, the GCRO will affirm the effectiveness of this Framework to the Board or Board-level committees. On behalf of the GCRO, the Global Head, ERM provides oversight of the effective implementation of this Framework through the evidence based self-assessment and affirmation of the RTFs from the RFOs to the GCRO.
- 14.2 The Global Head, ERM, on behalf of the GCRO, sets the FPGS for a common approach and mandatory requirements for Core Documents across the Group. The approach to Effectiveness Reviews and Regulatory Attestation is outlined in [Effectiveness Review Standard](#) (ERS).

- 14.3 The Global Head, Operational, Technology & Cyber Risk, on behalf of the GCRO, sets out a common approach for risk assessments across the organisation (RCSA) and approach to responding to Risk Events in the [Operational Risk Policy](#). The requirements for validation of internal control systems are set out in the Operational Risk Policy and Standard.
- 14.4 The RFOs will affirm the effectiveness of the RTFs to the GCRO through evidence based self-assessments. The Policy Owners will affirm the effectiveness of the Policies through evidence based self-assessments to the RFOs or the GCRO. As part of these effectiveness reviews, the Policy Owners should use the evidence gathered through both, the RCSA on the design and effectiveness of the supporting control environment, as well as from their own oversight and challenge activities. Standards linked directly to the ERMF, and RTFs (without policies) will have their effectiveness affirmed by the Standard Owners.
- 14.5 1LoD and / or Process Owners in both, the 1LoD and 2LoDs must validate and self-assess compliance to the control requirements, confirm the quality of validation, and provide evidence based self-assessments to the RFOs and Policy Owners on the adequacy of performance of their processes to the control requirements prescribed.
- 14.6 Those performing evidence based self-assessments (for internal purpose or for regulatory submission) are responsible for ensuring:
- The completeness of the requirements being self-assessed including the regulatory requirements from confirmed sources.
 - That the evidence-based response addresses the requirements.
 - That the supporting evidence for all the requirements is clearly documented.
 - That the conclusion on the level of compliance with requirements considers self-identified issues, audit-identified issues, gaps, remediation plans and evidence gathered through the RCSA or other validation reviews.
 - There is a maker-checker, and independent review of the response and compliance assessment, with review and challenge documented.
- 14.7 Material regulatory attestations are subject to sign-off by RFOs, Senior Managers (under the Senior Managers Regime) and / or an executive level committee with members comprising of Senior Managers or RFOs, prior to submission to the regulatory authority. Where appropriate:
- Legal should be engaged, along with Compliance, prior to commitment, to review the wording of material regulatory attestations.
 - Where the 2LoD is the attester, there should be adequate independence between the preparer and the reviewer to validate submissions.
- 14.8 Group Internal Audit provides independent assurance to the Board or Board-level committees on effectiveness of controls, and the systems of validation and review by the 1LoD and 2LoD.

15. Country Risk

- 15.1 The Global Head, ERM on behalf of the GCRO, will ensure there are annual and out-of-cycle country risk reviews with the local CEOs, and there is periodic reporting to senior management and Board on significant country risk events, issues and mitigation plans.
- 15.2 The Global Head, ERM ensures the Country Limits and Exposures are reasonable and in line with Group strategy, country strategy, and the operating environment, considering the identified risks. This includes economic, political, environmental and social risk factors under base and stressed conditions.
- 15.3 The monitoring of identified Country Risk exposures must be holistic and include foreign currency and local currency credit exposures to a particular country. The governance requirements are outlined in the [Country Risk Standard](#).

16. Risk Management for Branches and Subsidiaries

- 16.1 This Framework applies globally to all the Group's activities and applies to branches and subsidiaries.
- 16.2 Banking Subsidiaries must adopt the ERMF and RTFs and adjust as needed to comply with local laws and regulations. This would include review of the regulatory expectations on PRTs. The **Country**

Chief Risk Officer (CCRO) reviews whether variances to this Framework are required by local laws or regulations to be adopted locally and set local RA if needed. The CCRO must table amendments to the local risk management framework and RA at the country level governance arrangements. The country / local-level RFOs review whether variances to their respective RTFs are required by local laws or regulations to be adopted locally.

- 16.3 Local Regulatory Obligations: regulatory obligations to be implemented at a country-level may emanate from both Group-wide regulations and local regulatory authorities. The responsibilities for the various stages of the regulatory lifecycle are specified in Table 5 below.

Table 5: Regulatory lifecycle in countries

Activity	Responsibility in country
Identify material relevant regulatory authorities on an on-going basis	Country RFO or relevant Subject Matter Expert
Ensure completeness of regulatory authorities and ownership	Country CEO exercised through CNFRC
Ensure the identification of material new and amended laws and regulations issued by Financial Services Regulatory Authorities as and when issued	Country Head of CFCC
Ensure the identification of relevant new and amended laws and regulations issued by sources other than financial services regulators as and when issued	Country RFO or relevant Subject Matter Expert
Ensure all necessary documentation and audit trail exists for laws and regulations to demonstrate the process from identification through risk assessment, applicability assessment, dissemination to relevant 1LoD and to confirmation of implementation by the relevant 1LoD.	Country RFO or relevant Subject Matter Expert
2LoD oversight and challenge of the risks and controls identified	Relevant Country RFO or Subject Matter Expert

- 16.4 The Group requires visibility over the implementation status for all the country-level regulations beyond CFCC coverage. To help ensure holistic coverage, CFCC monitors confirmation of implementation for all regulations from Financial Services Regulatory Authorities regardless of RFO. Respective RFO (or delegates) are responsible to ensure timely implementation and manage risk associated with any overdue regulations pertaining to their PRT. The [Standard for Managing Regulatory Change by CFCC](#) provides further detail on the roles and responsibilities of CFCC, and respective RFOs (or delegates).
- 16.5 Where required by local regulator, or mandated in the ERGS, Branches must implement a **Country Risk Committee** (CRC) and Banking Subsidiaries must implement an **Executive Risk Committee** (ERC) to oversee the effective implementation of the ERMF locally. Appointing authorities are defined in the [Committee Governance Standard](#).
- 16.6 A set of RA and MTL metrics, as determined by the Group RFOs and ERM, should be allocated to material parts of the Group where risk is booked and managed, including material Group subsidiaries and branches, as defined in the [Risk Appetite Policy](#). CCROs are responsible for implementing and monitoring the metrics. Breaches will be escalated to the relevant CROs and Group RFOs.
- 16.7 The approach for Country / Local level ERMF review will follow the approach as outlined in the [Effectiveness Review Standard](#). Entities that formally adopt the Group ERMF (through local addendum or local Risk Management Framework) must perform a Country self-assessment to assess the overall adoption and effectiveness of the ERMF locally. The frequency applicability (annual or biennial) will be directed and communicated by the Effectiveness Review Standard Owner prior to the commencement of the Country ERMF Effectiveness review exercise.
- 16.8 The CCRO (or delegate) is responsible for ensuring the completion of the self-assessment and tabling the results at the local risk committee for discussion. The results of the self-assessment will be considered in the Group Effectiveness Review.

- 16.9 This Framework applies as well to non-Banking subsidiaries¹⁹ that should follow the principles of the ERMF and ensure that key local risks are identified and effectively managed. No formal adoption of the ERMF is required, unless guided otherwise by local laws and regulations.
- 16.10 The Global Head, ERM sets governance standards for branch and subsidiary level implementation of this Framework through the [Entity Risk Governance Standards](#) (ERGS).

----- END OF PART A -----

¹⁹ Non-Banking Subsidiaries also include Significant Non-Banking Subsidiaries. For corporate governance of non-banking subsidiaries and significant non-banking subsidiaries, refer [here](#).

Part B

Risk Type Frameworks

Chapter One

1. General Principles and Governance

1.1 The following principles apply in relation to the purpose, governance, and structure of the RTFs included in Part B of this Framework.

a) Purpose and Content

- The purpose of RTFs is for the RFO to outline any unique risk management approach of the PRT for the GCRO, internal stakeholders (Management Team, Senior Managers, other RFOs, and the third LoD) and external stakeholders (Board members, external auditors and regulators). The RTFs must be read in conjunction with the policies and standards mapped to the ERMF as outlined in the appendices in Part C.
- The RTFs are built on a risk-based approach, meaning the risk management plans, processes, activities, and resource allocations are determined in accordance with the level of risk. The RTFs considers processes and tools that are forward-looking, they should be repeatable, sustainable and anticipate future needs.
- The first 1LoD must give due consideration to the apparent risks at the point of strategic choices, decision making and the management of conduct risk.

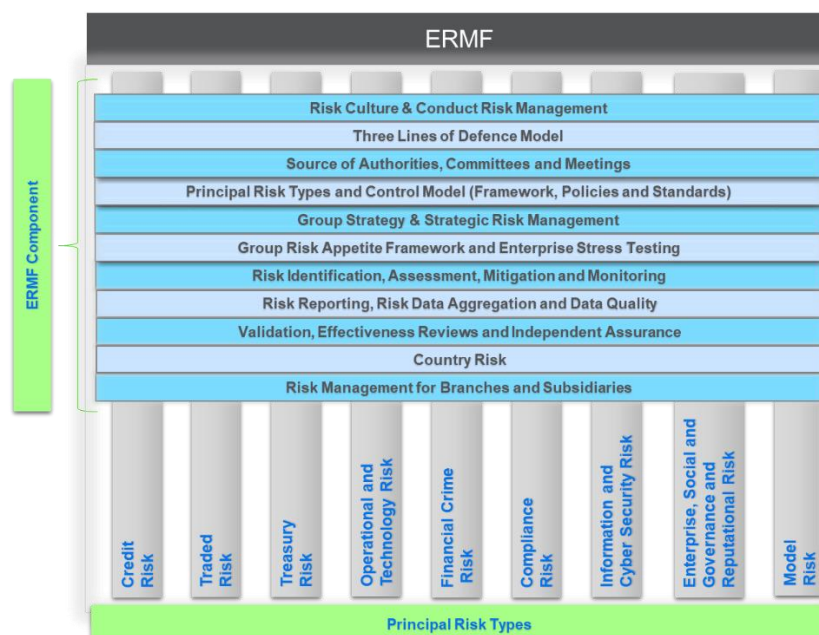
b) Governance and Decision Making

- The Group allocates responsibilities for the RTFs in a manner consistent with the three LoD outlined in Part A under Section 4 and 8.
- The GCRO has delegated RFO's responsibilities associated with the PRTs to the individuals identified in each RTF and Table 2 (Part A). The RFO periodically reviews the RTF, at a minimum every two years, or earlier if triggered by any material change in circumstances.
- The RTFs are the formal mechanism through which the delegation of PRT authorities is set out. The RFOs delegates risk authorities to designated individuals for the management of their PRT, which may include the responsibility for writing, maintaining and approving policies / standards and for 2LoD oversight and challenge at a global business, product and function level as well as country level. Any unique delegation and governance requirements are outlined within the respective RTF chapter where applicable.

c) Structure

Whilst the RTFs include the unique requirements applicable to each PRT's risk management approach, these must be read in conjunction with other components of the ERMF (refer to figure 1) as outlined in Part A and B, the underlying policies and standards, including:

Figure 1: Enterprise Risk Management Framework Components



- Conduct Risk Management in Section 4 (Part A), to ensure that the relevant Conduct Outcomes are achieved through risk identification, control, monitoring and governance arrangements.
- Risk Appetite in Section 10 (Part A), to ensure that the RFOs review at least annually the adequacy and effectiveness of the Group RAS, metrics and thresholds, and propose changes to Global Head, ERM and the GCRO as necessary. For more information on the allocation of Group RA, monitoring and escalation, refer to the [Risk Appetite Policy](#) and [Standards](#).
- Enterprise Risk identification, assessment, mitigation and monitoring in Section 11 (Part A), to ensure that the risk identification, assessment, mitigation and monitoring is performed in line with the principles set out in this Framework, the RCSA and Response Management requirements set out in the Group [Operational Risk Policy](#) and [Standards](#). Unique requirements can be referred to within the PRTs related policies, including the requirements for specific skills training and accreditation.
- Enterprise Stress Testing in Section 12 (Part A), to ensure any required PRT specific stress testing or sensitivity analysis to assess vulnerabilities under stressed conditions are documented and implemented. Additionally, Credit Risk, Traded Risk and Operational & Technology Risk are subject to minimum capital requirements in accordance with the UK Capital Requirements Regulation (UK CRR), for the Group to operate within Risk Capacity. At Group and Solo¹ level, Risk Capacity consists of Pillar 1 and 2A requirements. For all other PRTs there are no Pillar 1 minimum requirements in accordance with the UK CRR, but these are considered as part of Operational Risk for Pillar 1.
- Risk reporting, risk data aggregation and data quality in Section 13 (Part A), to ensure adherence to the requirements outlined in the [Group's Risk Data Aggregation Standards](#), [Risk Reporting Standards](#) and [Data Quality Management Standards](#) in the end-to-end process of defining, gathering, and processing of risk data to meet the Group's risk reporting requirements.
- Effectiveness review in Section 14 (Part A), to ensure that the Effectiveness Review of RTFs follows an evidence-based approach. Further details are included in the [Effectiveness Review Standard](#).
- Regional and local implementation in Section 16 (Part A), to ensure the Group RFO appoints local RFO for the management of PRTs locally and delegates authorities required to discharge their responsibilities. The local RFO is responsible for ensuring branch or subsidiary compliance with the requirements set out in the RTFs. All SCB branches and banking subsidiaries including Hubs must implement ERMF through a local addendum and comply with the requirements set out in the [ERGS](#), including any variations to the RTFs. The RTFs applies to non-banking subsidiaries for its relevant risks. Where applicable, non-banking subsidiaries should follow the principles of the PRT and ensure that key local risks are identified and effectively managed. No formal implementation of the RTFs is required, unless guided otherwise by local laws and regulations.
- Crisis Management: For more information, please refer to the [Group Client Service Resilience Policy](#) and underlying Standards. A crisis may arise from a variety of reasons and must be escalated to the respective business/segment to relevant country, regional and Group stakeholders and managed as per the escalation requirements set within the relevant standards.
- Breach and escalation mechanism: The RFOs are responsible for developing a breach and escalation mechanism for issues determined to be material by the RFO. RFOs are required to escalate to compliance function all regulatory issues and breaches rated medium or above on the **Group Risk Assessment Matrix** (GRAM) and all regulatory penalties or enforcement action from Financial Services Regulators regardless of risk rating. Escalation of breaches must be aligned with the response management requirements set out in the [Group Operational Risk Policy](#) and

¹ Solo is a regulatory construct for the purposes of capital and liquidity, comprising of a sub-set of entities within SC Bank and comprises SCB UK, foreign branches of SCB UK and subsidiaries which the PRA allows us to consolidate.

Solo is regulated by the PRA meaning it must meet regulatory minimum requirements for capital and liquidity. For the subsidiaries consolidated as part of Solo under a PRA permission, we are required to demonstrate no impediment to the movement of capital and liquidity between SCB UK and these subsidiaries.

[Standards](#). Instances of material non-compliance to this RTFs, related policies and/or standards must be escalated to the RFO or their delegates.

- Other areas of risk: The RFO is required to demonstrate in the RTFs, policies and/or standards how these risks are considered. The Policy Owners for such risk may sit independently with distinct policies that cut across multiple PRTs. Where applicable, policies that are linked directly to the ERMF as listed in Part C, such as Climate Risk and Digital Asset policies, are in scope of the RTFs.

Please refer to Part C for common appendices in scope of all the RTFs.

TREASURY RISK TYPE FRAMEWORK

Chapter Number	Two – Part B of the ERMF
Principal Risk Type	Treasury Risk
Risk Framework Owner Name	Jason Forrester
Risk Framework Owner Job Title	Global Head ERM & Deputy CRO SC Bank
Document Contact Name	Rehan Qudratullah
Document Contact Job Title	Interim Treasury Chief Risk Officer
Version Number	1.2

Contents

1. Overview of the Treasury Risk Type Framework.....	3
1.1 Treasury Risk management principles	3
2. Three Line of Defence Roles and Responsibility & Governance Committee Oversight	4
3. Decision Making Authority and Delegation.....	5
4. Regulatory Obligations and Escalation Mechanism	6
4.1 Group-wide Regulatory Obligations	6
4.2 Country-level Regulatory Obligations.....	7
4.3 Breach and escalation mechanism	8
5. Risk Appetite	8
6. Risk Reporting, Risk Data Aggregation and Data Quality.....	9
7. Enterprise Stress Testing, Capital and Liquidity Adequacy	9
7.1 Stress Testing.....	9
7.2 Capital and Liquidity Adequacy.....	10
8. Effectiveness Review and Quality of Implementation	11
Appendix B: Version Control.....	12

Version Control Table

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Isil Kilic	<p>Approval level for the cascaded PV01 limit for Fair Value portfolio has been highlighted as the respective Regional Traded Risk Management Heads.</p> <p>Refence to Prudential Compliance Framework (PCF) has been removed.</p> <p>The change in risk committees has been reflected in Figure 2.</p> <p>Appendix A has been removed given the standards directly linked to the Treasury RTF have already been included in Part C of the ERMF for common appendices.</p>	Non-material	Jason Forrester	1.2	5 Dec 2024

The full version history is included in the RTF [Appendix B](#).

Chapter Two

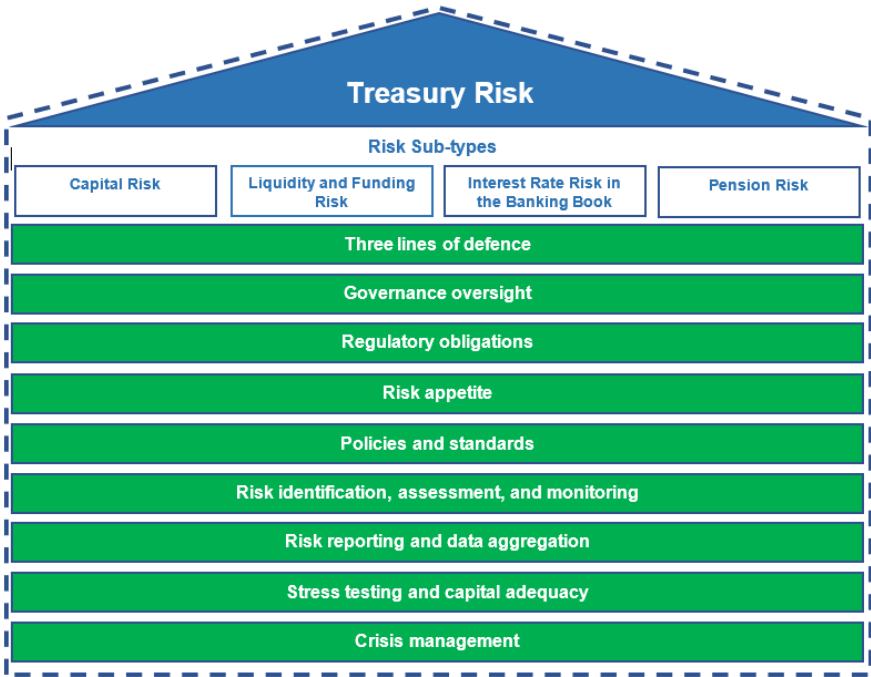
1. Overview of the Treasury Risk Type Framework

1.1 Treasury Risk management principles

Treasury RTF (this Chapter) is managed across the Group in line with the following risk management principles:

- Maintain sufficient levels of capital and ensure **Minimum Requirements for own funds and Eligible Liabilities** (MREL) are met, commensurate with business strategy and risk profile for both **business-as-usual** (BAU) conditions and market / idiosyncratic stress.
- Ensure appropriate composition and distribution of capital and MREL to support business activities.
- Hold adequate levels of liquid resources to meet payment obligations, including intra-day, for both BAU conditions and market / idiosyncratic stress.
- Conduct appropriate scenario testing, reverse stress testing and any other scenario modelling to help calibrate appropriate levels of capital and liquidity and to understand the potential impact to the business from emerging risks.
- Ensure an appropriate funding profile and diversified sources of both unsecured and secured funding from both a counterparty and industry perspective.
- Manage the liquidity portfolio within risk appetite to protect the liquidity of the Group whilst optimising for cost of funding and charging out the costs of liquidity and capital appropriately across the business lines.
- Ensure potential loss of earnings or economic value due to adverse movements in interest rates and foreign exchange rates are appropriately captured, measured, and managed.
- Maintain a usable set of contingent capital and liquidity actions options in relation to BAU, recovery and resolution.
- Ensure compliance with applicable regulations pertaining to Capital Risk, Liquidity and Funding Risk, **Interest Rate Risk in the Banking Book** (IRRBB), Recovery and Resolution Planning and Pension Risk.
- Monitor Climate Risk, Third Party Risk and Digital Asset Risk profile associated with Treasury Risk and provide remediation action plans as applicable.

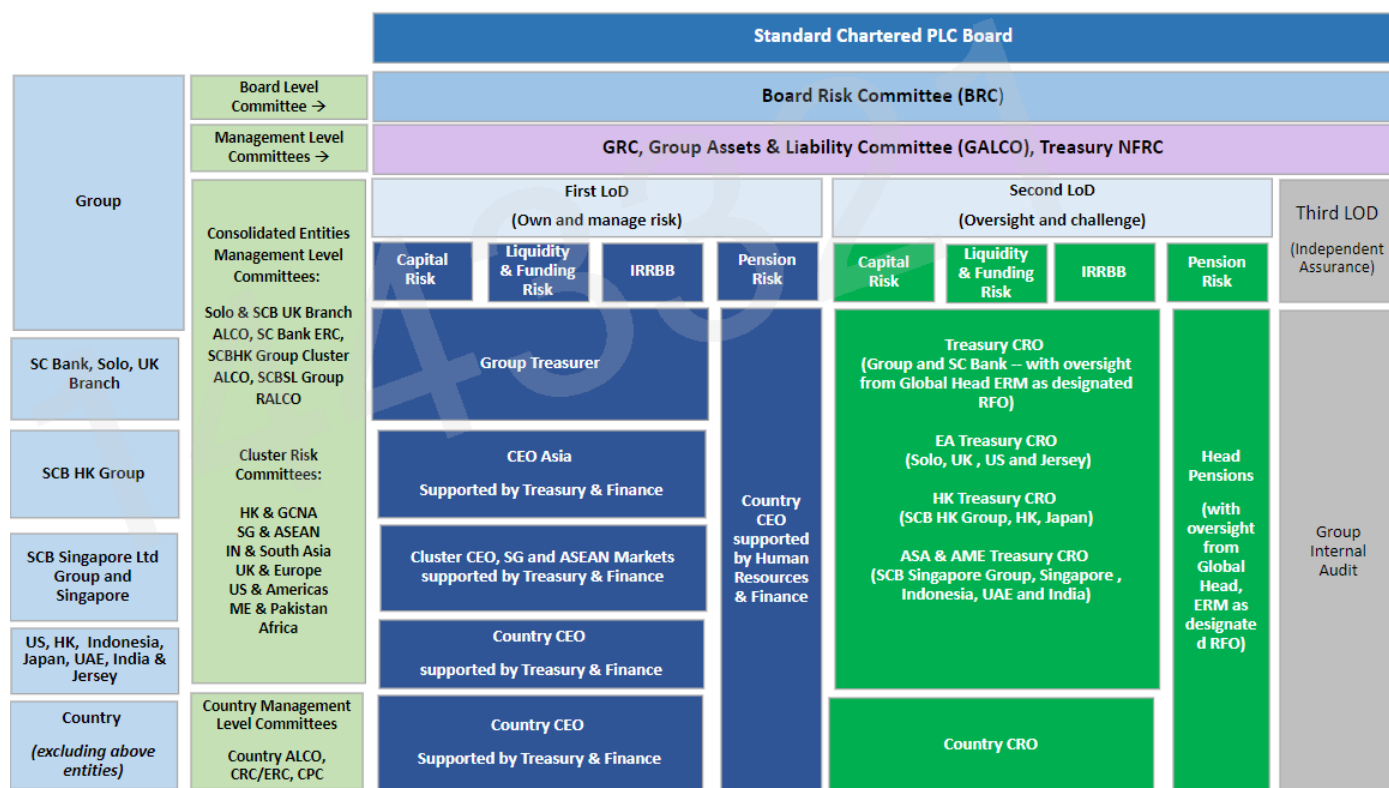
Figure 1: Treasury Risk overview



2. Three Line of Defence Roles and Responsibility & Governance Committee Oversight

In line with the three LoD model, the detailed set of Global, Hub and Country-level roles and responsibilities for managing Treasury Risk across the 1LoD and 2LoD are provided in Figure 2 below.

Figure 2: Treasury Risk – Overview of the Three Lines of Defence & Committee Governance



* In line with the local regulations, Country CROs will be the second LoD for the following countries: Germany, China, Korea, Taiwan, Thailand, Vietnam, and Malaysia. They will be supported by the Regional Treasury CROs.

The **Group Chief Financial Officer (GCFO)** has responsibility for management of the financial resources of the Group under the Senior Managers Regime.

1LoD responsibilities specific to Treasury Risk are outlined below:

- Forecast and propose Board Risk Appetite metrics, **Management Team (MT)** limits and **Management Action Triggers (MATs)**.
- Manage Treasury Risk exposures within Risk Appetite, limits, and MATs.
- Forecast and manage the high-quality liquid assets to ensure the Group is adequately funded, in the required currency to meet its obligations and client funding needs.
- Maintain market access for funding and centralise any liquidity generation from a central bank window either in BAU or stress, via the use of security or non-security collateral.
- Ensure through the Group's annual corporate planning process / funding plan that the capital, liquidity & funding and IRRBB remain within Risk Appetite levels.
- Implement and comply with regulatory requirements.
- Own and approve standards to manage Treasury Risk in line with the requirements set out in this Chapter and related policies.
- Own the **Expected Credit Loss (ECL)** calculation for Treasury exposures.
- Propose limit frameworks for review by **Treasury Chief Risk Officer (CRO)** and cascade them through the Group.
- Implement and monitor policy requirements, metrics, Risk Appetite, limits, and MATs with appropriate escalation processes in place.
- Escalate significant risks and issues to the second LoD promptly.

- Own, develop, and maintain models and perform related model risk life cycle activities linked to these responsibilities with the support of the Model Validation Team.
- Ensure an effective transfer of liquidity valuation and interest rate risks between the business and Treasury Markets, including through proposing and implementing the Funds Transfer Pricing methodology.
- Ensure all alternative management actions have been considered including examining risk weighted asset growth rates and returns to conserve capital resources and effectively manage the Group's capital ratios.
- Ensure relevant components of recovery and resolution plans are updated for capital and liquidity management actions to survive relevant stress.
- Assess and manage material financial and non-financial risks in respect of pensions.

2LoD responsibilities specific to Treasury Risk are outlined below.

- Own and approve policies to manage capital, liquidity, funding, and IRRBB risks.
- Review and challenge the Risk Appetite and the framework setting MATs and the level of the thresholds established (including temporary limit extensions)¹.
- Review and challenge the Funds Transfer Pricing methodology as part of GALCO review.
- Review and challenge the capital, liquidity & funding and IRRBB risk assessment of the corporate plan as part of ALCO review.
- Review and challenge 1LoD's regulatory interpretations and regulatory attestations of financial regulatory obligations, supporting the annual prudential compliance attestation of the chapters owned by Treasury.
- Review and challenge the results of independent validations of Treasury models by Group Model Validation.
- Review and challenge Treasury Risk related sections and have holistic oversight of regulatory stress tests including the Bank of England Annual Cyclical Scenario, **Internal Capital Adequacy Assessment Process** (ICAAP), **Internal Liquidity Assessment Process** (ILAAP) and Recovery Planning Stress Tests. Provide a comprehensive view of 2LoD challenge to senior group committees, as appropriate.
- Review and challenge of Treasury ECL.
- Escalate significant risks and issues and ensure appropriate management actions are taken to mitigate their impact. Ensure such events are recorded in the appropriate reporting system.
- Provide holistic oversight over the resolvability self-assessments; review and challenge the resolvability assessment for Treasury barriers; assess recovery and resolution planning testing including holistic simulation-based testing exercises involving the Board, Management Teams, and **Crisis Management Groups** (CrMGs) at a group and country level.
- Review and challenge of Pension Risk stress test results, governance, and funding requirement of pension plans.

Third Line independently assesses whether First and Second LoD controls and risk management processes are effective as set out in Part A of the ERMF

3. Decision Making Authority and Delegation

The Treasury RTF is the formal mechanism through which the delegation of Treasury Risk authorities is made in addition to job descriptions and the **Group Delegated Authorities Manual** (GDAM). The Global Head, ERM delegates authorities to designated individuals through this Chapter.

The Global Head, ERM delegates authorities to effectively implement this framework to:

- the Treasury CRO for Capital Risk, Liquidity and Funding Risk and IRRBB,
- to the Head, Pensions for Pension Risk.

¹ Including the limit framework for Treasury Markets and Treasury Capital interest rate management (e.g. PV01 set by Traded Risk Management and CR01 set by Credit Risk)

The Global Head, ERM retains authority and accountability for affirming effectiveness of the RTF to the GCRO (see Section 14 of ERMF main chapter).

Responsibilities for Treasury limit setting:

The Board Risk Appetite Metrics and the Management Team limits for Treasury Risks are approved by the relevant governance committee in line with the Risk Appetite Policy. Treasury CRO reviews and challenges the proposal prior to submission to the relevant governance committee for approval.

Capital

- The Head of Capital Management recommends Capital Risk Appetite and cascades the approved Risk Appetite set to regional and/or country level where applicable.
- Capital management decision authorities and delegations are set out in the GDAM. This details the delegated authorities for changes to corporate structure, internal capital injections, profit retentions, external issuance and the repurchase of regulatory capital instruments.

Liquidity

- The Global Head, Treasury Liquidity recommends Risk Appetite and cascades the approved Risk Appetite to regional level where applicable, in accordance with the MAT frameworks approved by Treasury CRO.
- The Global Head Treasury Liquidity sets framework for internal metrics and sets regional MATs for Risk Appetite.
- The Regional Treasurers have authority to cascade down their regional MATs to the countries in their regions as well as setting MATs for other internal metrics within agreed parameters.
- The operational procedures in relation to limit setting and cascading to regions/countries can be found in the [Liquidity Limits Management and Escalation Standard](#).

IRRBB

- Global Head, Treasury Liquidity recommends IRRBB Risk Appetite excluding PV01 limits, and cascades Group limits to regional and/or country level where applicable.
- The Global Head, Treasury Markets recommends net PV01 limits across fair value and banking book portfolios, and cascades Group limits to regional and/or country/entity level where applicable (i.e. PV01 limit for combined Fair Value and Amortised Cost portfolio is approved by Treasury CRO, and PV01 limit for Fair Value portfolio by Traded RFO for the Group and by the respective Regional Traded Risk Management Heads for the cascaded metrics).
- Treasury CRO reviews and approves the proposed limits.

Regional or Country Prudential Limits

- Internal limits to comply with regional or country prudential limits are proposed by Regional Treasurers and are approved in line with local governance requirements.
- Local governance requirements may require the Risk Appetite to be approved by local Board or ALCO.

Intragroup Credit Limits

- Treasury CRO sets the framework for Intragroup credit limits i.e. from Solo to subsidiaries, from subsidiaries to Solo, and from subsidiaries to subsidiaries. The decision authorities and delegations can be found in [Intragroup Accounts Standard](#).

4. Regulatory Obligations and Escalation Mechanism

4.1 Group-wide Regulatory Obligations

The table below outlines the subject matter experts who are responsible for ensuring implementation and compliance with all regulatory obligations associated with their respective area of responsibility.

Table 1: Responsible SMEs

Area of Law and Regulation	SME / Owner
Prudential - Capital	Group Treasurer
Prudential - Liquidity	Group Treasurer
IRRBB	Group Treasurer
Recovery and Resolution planning	Group Treasurer
Pension Risk	Head, Pensions

For regulations issued by financial services regulators, the Conduct, Financial Crime, Compliance function will identify new and amended regulations as and when issued and communicate the relevant regulatory obligations to the applicable RFO delegate.

The Group Treasurer (or delegate) is responsible for:

- providing input for documenting in this Chapter all areas of Treasury Risk related regulations, to be applied Group-wide which they are responsible for.
- identifying regulatory authorities in all countries where the Group operates who may issue regulations relevant to the Group for the areas of regulations within the Treasury Chapter.
- identifying material regulations relevant to the Group issued by those regulatory authorities.
- including relevant regulation in standards where necessary, to ensure the Group meets regulatory requirements.
- providing input for documenting relevant regulation in policies where necessary.
- overseeing and monitoring implementation of those standards.
- maintaining adequate audit trail documentation to demonstrate material regulations have been identified and implemented; and
- ensuring sign-off for material regulatory attestations.

The Treasury CRO is responsible for:

- documenting in this Chapter all areas of Treasury Risk related regulations, to be applied Group-wide
- including relevant regulation in policies where necessary, to ensure the Group meets regulatory requirements.
- overseeing and monitoring implementation of those policies.
- providing oversight and challenge of the risks and controls identified to meet the prudential regulatory obligations.
- reviewing and challenging 1LoD's regulatory interpretations and regulatory attestations regarding financial regulatory obligations supporting the annual prudential compliance attestation of the chapters owned by Treasury.

4.2 Country-level Regulatory Obligations

Regulatory obligations to be implemented at a country-level may emanate from both extra territorial regulations and local regulatory authorities.

The CEOs are responsible for ensuring implementation and compliance with all local prudential capital, liquidity, IRRBB, pension risk and recovery and resolution planning laws and regulations, as set out in section 2 figure 2.

The responsibilities for the various stages of the regulatory lifecycle are specified in the table 2 below.

Table 2: Regulatory life cycle and country level responsibility

Activity	Responsibility in country
Identify material relevant regulatory authorities on an on-going basis.	Country CFO
Ensure completeness of regulatory authorities and ownership.	Country CEO exercised through CNFRC
Ensure the identification of material new and amended laws and regulations issued by financial services regulator authorities as and when issued.	Country Head of CFCC
Ensure the identification of relevant new and amended laws and regulations issued by sources ² other than financial services regulators as and when issued.	Country CFO
Ensure all necessary documentation and audit trail exists for laws and regulations to demonstrate the process from identification through risk assessment, dissemination to relevant 1LoD applicability assessment and to confirmation of implementation by the relevant 1LoD.	Country CFO
2LoD oversight and challenge of the risks and controls identified **.	Country CRO*

* In conjunction with Regional Treasury CRO

** The 2LoD oversight and challenge does not cover the risk ownership of local regulations. Country CRO / Regional Treasury CRO only acts in advisory capacity where the 1LoD needs it.

The [Standard for Managing Regulatory Change by CFCC](#) provides further detail on the roles and responsibilities of CFCC and respective RFOs (or delegates).

The Group requires visibility over the implementation status for all the country-level regulations beyond CFCC coverage. To help ensure holistic coverage, CFCC monitors confirmation of implementation for all regulations from Financial Services Regulatory Authorities regardless of RFO. Respective RFO (or delegates) and for Treasury Risk, Country CFO (or delegate) are responsible to ensure timely implementation and manage risk associated with any overdue regulations pertaining to their PRT.

4.3 Breach and escalation mechanism

The Treasury CRO is responsible for developing a breach and escalation mechanism for issues determined to be material.

The chapter owners for prudential compliance attestation must escalate all material instances of non-compliance to the relevant Governance Committees and **Treasury Non-Financial Risk Committee** (TNFRC), to Compliance, and confirm that the regulator was informed where needed.

5. Risk Appetite

Details of Risk Appetite allocation, monitoring and escalation process can be found in the relevant policies and standards for each sub risk type:

- Capital Management Policy and Capital Risk Appetite Standard (for Capital Risk)
- Liquidity and Funding Risk Policy and Liquidity Limits Management and Escalation Standard (for Liquidity and Funding Risk)
- IRRBB Policy and IRRBB Standard (for IRRBB) and Pension Risk Standard (for Pension Risk)

² For example, employment regulations issued in Singapore by the Ministry of Manpower

6. Risk Reporting, Risk Data Aggregation and Data Quality

The Global Head, ERM relies on the respective Treasury and Finance leads and Head of Pensions for outlining risk data aggregation, risk reporting and data quality requirements and implementing those requirements in accordance with the [Risk Reporting Standards](#) (RRS), [Risk Data Aggregation Standards](#) (RDAS) and [Group Data Quality Management Standards](#) (DQMS). Those responsible for the priority reports are listed in Part C of the ERMF.

7. Enterprise Stress Testing, Capital and Liquidity Adequacy

7.1 Stress Testing

Capital Risk

Stress tests are performed at least annually in support of regulatory requirements (e.g. ICAAPs and industry wide stress tests) and to inform the Group's capital adequacy assessment and Capital Risk Appetite calibration, explore business vulnerabilities and support Enterprise Risk Management, Group strategy and Group planning. These stress tests are designed to assess the ability of the Group, Solo, regional hubs, and countries to continue to meet their capital requirements during a severe but plausible stress and to inform management decision making. Where scenarios are not prescribed by regulators, they should be sufficiently severe and linked to the Risk Identification process to ensure that they consider the most material risks and uncertainties to the Group's balance sheet and/or business models.

All regulatory Group and Solo capital stress tests are performed in compliance with the processes and governance defined by the [Enterprise Stress Testing Policy](#). Management stress tests are also run to inform Group planning and assess the impact of principal risks and uncertainties on the Group's and countries' operations, based on less extreme and more plausible events.

Stress tests relating to the Group, Solo, hubs and country ICAAPs are detailed in the ICAAP Standard.

Climate Risk may be assessed through targeted stress tests set by Group and local regulators. For example, the 2021 Bank of England Biennial Exploratory Scenario was focused on Climate Risk. The results of any such targeted stress test may be used to inform the Climate Risk P2A assessment.

Liquidity and Funding Risk

Stress tests are performed daily, designed to help the Group plan for severe but plausible stress and to inform the Group on whether it has adequate liquidity resources commensurate with its business model and balance sheet shape and size. Ad hoc stress tests in country may be requested by regulators and management.

All stress tests are performed in compliance with the [Liquidity and Funding Risk Policy](#), [Liquidity Stress Testing Standard](#) and [Liquidity Coverage Ratio Standard](#).

Stress tests relating to the Group and Solo ILAAP are detailed below and in the Stress Testing Standards.

Interest Rate Risk in the Banking Book

Stress tests are performed monthly to identify structural risks to Net Interest Income or the Economic Value of the Banking Book under adverse but plausible interest rate scenarios. Additionally, stress testing of IRRBB is covered as part of ICAAP and BoE concurrent stress testing exercises to ensure that the Group, Solo and countries continue to meet their capital requirements during a severe but plausible stress. Stress testing of price risk on Fair Value instruments in the Banking Book is conducted by Traded Risk Management under the Market Risk Framework.

Recovery Planning

Recovery Plan includes four stress test scenarios for formal submissions and can vary during maintenance cycles. The plan is reviewed annually to ensure it is up to date. The Recovery Plan stress testing is conducted annually, and it is used to demonstrate that the Bank's Recovery Plan is suitable for use in a range of distinct types of stress and test how different elements of the plan (such as indicators, governance and management actions) would interact in these stresses. These scenarios are designed to bring the Group close to the **Point of Non-Viability** (PONV) and includes deploying management actions aimed to restore the Group's capital and liquidity indicators to appropriate levels. In line with regulatory guidance,

recovery plan scenario testing considers the impact of market-wide, idiosyncratic, and joint events. The Recovery Plan stress testing is also conducted in countries, where, mandated by local supervisory authorities. The governance process follows the requirements set out in the [Reverse Stress Test and Recovery Plan Stress Test Standard](#), which is mapped to the [Enterprise Stress Testing Policy](#).

Reverse stress tests

Reverse stress tests are run annually as part of the ICAAP process for the Group, Solo and for countries, where this is a local regulatory requirement. These tests are focused on exploring how business model vulnerabilities may lead to the PONV i.e. the point at which the market loses confidence in a firm and, as a result, the firm is no longer able to conduct its business activities in the absence of a resolution. Where the risk of reaching PONV is judged to be unacceptably high, mitigating action is taken to reduce the likelihood of the event occurring and/ or the scale of the impact. This may involve setting aside additional capital or liquidity.

Resolution planning

Resolution planning involves testing at a barrier playbook level conducted annually, as well as holistically through simulations.

Resolution barrier capabilities are evaluated as part of resolution planning to assess the Group's ability to execute processes and activities in the event of resolution.

All barrier-level testing is carried out in compliance with the [Resolution Standard](#) that set out the approach and methodology adopted for testing resolution-based capabilities and arrangements to validate the state of the Group's resolvability and readiness to execute its preferred resolution strategy.

Simulation-based exercises with the Board, MT and various other crisis fora including CrMGs and response teams are conducted to holistically evaluate the ability of the Group to deploy several barrier level capabilities and arrangements as needed over the resolution stress continuum to meet resolvability outcomes.

Such holistic, simulation-based exercises that cover multiple resolution barriers within its scope, involve a resolution scenario covering a wide range of extreme events leading to failure and define a specific period across the stylised resolution timeline to highlight the interconnectedness between barriers. Where possible, existing scenarios used in other stress tests for e.g., reverse stress test, that meet the profile of a resolution scenario, are leveraged to run the simulation-based exercises.

The holistic exercises with the Board separately aim to assess the efficacy of the master resolution playbook in clarifying how governance arrangements are expected to support Board decision making and interaction with subsidiaries boards in the lead up to resolution.

Both barrier playbook level tests and holistic exercises are overseen and assessed by independent observers including Risk (Treasury CRO).

Pension Risk

Pension Risk is included in the following regulatory tests:

- BoE & ICAAP 2B - a five-year projection is applied across the Group
- ICAAP 2A – as required by the PRA, a 1-in-200-year severity stress test that specifically targets pension metrics adversely.

Pensions are also included in recovery planning.

7.2 Capital and Liquidity Adequacy

Capital Adequacy

Capital Risk is subject to minimum requirements in accordance with the UK **Capital Requirements Regulation (CRR)**.

- At Group and Solo level, minimum requirements arise from Pillar 1 and 2A requirements. An assessment of the Pillar 2A risks (i.e. risks that are not covered, or not sufficiently covered, by Pillar 1) is undertaken annually as part of the ICAAP. The assessment forms the basis for the Regulator's **Supervisory Review and Evaluation Process (SREP)** which together with the Pillar 1 CRR minimum

requirements, determines the Group's **Total Capital Requirement (TCR)**. Firms are expected to maintain financial resources at or above the level specified in the TCR at all times.

- IRRBB is captured within the Pillar 2A assessment which evaluates the potential for loss from adverse movements in interest rates on the banking book. Treasury is responsible for assessing capital requirements associated with yield curve and swap spread basis risk from banking book positions, residual basis risk that remains with the business and customer optionality.
- At a Group and Solo level, the Pillar 2 assessment for Capital Risk is managed by the Treasury Capital team. Local regulators may have an approach that varies slightly to the above, in which case local regulations must be followed.

In addition to the ICAAP, day-to-day capital management activities also ensure that the Group's capital, leverage and MREL position is managed within the Board-approved Capital and MREL Risk Appetite, respectively. There are broadly four processes.

1. Capital forecasting and allocation. The Corporate Plan covers strategic business and capital plans across a five-year horizon. It is approved by the Board annually in November/December. Refer to the Capital and Leverage Forecasting Standard for details.
2. Capital deployment. Outside the budgeting process, capital is allocated to countries through capital retentions and injections (or local non-equity issuance if approved by Group) and is subject to the Capital Deployment Standard.
3. Capital supply. The capital issuance plan is presented to GALCO in January for the upcoming year, with a mid-year review. The Group seeks to maintain a strong capital base, including non-equity capital issuance, to support its strategy and business plans and to meet regulatory capital, leverage and loss absorbing capacity requirements. Refer to the Capital and Leverage Forecasting Standard for details.
4. Local capital management. The Group is required to manage capital by legal entity and its branches. The Country first LoD for Capital Risk must ensure processes are in place to monitor and ensure compliance with local regulatory requirements and Risk Appetite, with appropriate oversight from the Country second LoD. Country ALCOs play a critical role in the day-to-day management of the balance sheet and making capital allocation trade-offs within the constraints of their respective balance sheets.

Liquidity Adequacy

Liquidity and Funding Risk is subject to Pillar 1 minimum requirements in accordance with the UK CRR. The Liquidity and Funding Risk Pillar 1 requirement is determined by the regulator, a risk appetite is set above the minimum requirement and cascaded to countries as limits and MATs.

In accordance with the **Overall Liquidity Adequacy Rule (OLAR)**, an ILAAP is undertaken annually. OLAR requires firms to always maintain adequate liquidity resources, both as to amount and quality, to ensure that there is no significant risk that its liabilities cannot be met as they fall due.

The ILAAP has captured an assessment of two key components in this document.

- an approach to manage liquidity and funding risks covering policies, procedures, metrics, and governance arrangements and
- the Board Risk Appetite including stress testing scenario, assumptions and results used to meet the OLAR.

The Pillar 2 requirements for Liquidity and Funding Risk are set by the regulator at Group and Solo level. Pillar 2 requirements are cascaded to countries as limits and MATs where appropriate.

8. Effectiveness Review and Quality of Implementation

The Effectiveness Review for the Treasury RTF will be performed by Treasury with oversight from Treasury CRO. The Global Head, ERM as RFO will affirm the effectiveness of the RTF to the GCRO annually.

Appendix B: Version Control

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Zeeshan Arif	Initial version created as part of the consolidation of standalone RTFs during the ERMF/RTF simplification exercise.	Material	SC PLC Board	1.0	7 Dec 2023
Renzo Baio	Updated Figure 2: Overview of the three Lines of Defence to reflect organizational changes for CIB Credit and updated Standards linked to the RTF (Appendix A). ERMF Part C: <ul style="list-style-type: none">• C2 Appendix: Removal of Funds Transfer Pricing policy (To be retired)• C3 Appendix: Addition of 4 Priority reports and correction of OBSC to OBSF• C5 Appendix: Addition of Banking Book Funds Transfer Pricing (FTP) Standard and removal of Private Banking and FM Legal entity booking model standards	Non-Material	Jason Forrester	1.1	20 May 2024
Isil Kilic	Approval level for the cascaded PV01 limit for Fair Value portfolio has been highlighted as the respective Regional Traded Risk Management Heads. Refence to Prudential Compliance Framework (PCF) has been removed. The change in risk committees has been reflected in Figure 2. Appendix A has been removed given the standards directly linked to the Treasury RTF have already been included in Part C of the ERMF for common appendices.	Non-material	Jason Forrester	1.2	5 Dec 2024

Note: Please refer to Part C of the ERMF for common appendices.

----- END OF CHAPTER TWO -----

CIB CREDIT RISK TYPE FRAMEWORK

Chapter Number	Three – Part B of the ERMF
Principal Risk Type	CIB Credit Risk
Risk Framework Owner Name	Shivkumar Mahadevan
Risk Framework Owner Job Title	Co-Head-CRO, CIB and CRO, ASEAN & South Asia
Document Contact Name	Christina Khoo Swee Lee
Document Contact Job Title	Head, Policy and Process, CIB
Version Number	1.3

Delegation

For non-material changes to RTF	
Name	Christina Khoo Swee Lee
Job Title	Head, Policy & Process - CIB

Contents

1. Overview of the CIB Credit Risk Type Framework	3
1.1 CIB Credit Risk related principles	3
1.2 Overview of CIB Credit Type Framework	3
1.3 Updates to Credit Risk Type Framework	4
2. Three Line of Defence Roles and Responsibility and Governance Committee Oversight	5
3. Decision Making Authority and Delegation	6
4. Dynamic Risk Identification	7
5. Regulatory Obligations and Escalation Mechanism	7
5.1 Group-level Regulatory Obligations	7
5.2 Breach and escalation mechanism	8
6. Capital Adequacy	8
7. Skills Training and Accreditation	8
Appendices specific to this Framework	9
Appendix A - Credit Risk references to Climate Risk, Digital Asset Risk and Third-Party Management Risk	9
Appendix B - CIB Credit Risk 2LoD processes	10
Appendix C - CIB Credit Risk 2LoD process owners	10
Appendix D - SAR 2LoD process owners	13
Appendix E - Credit Risk references to other RTFs	15
Appendix F - Risk Reporting	15
Appendix G – Version Control	16

Version Control Table

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Oki Darvian	Part B – CIB Credit RTF. <ul style="list-style-type: none"> Amend 'CRO, CIB' title to 'Co-Head – CRO, CIB' Figure 2: Update to the Banks committee names Section 3: <ul style="list-style-type: none"> Update to Client-segment Level Credit Sanctioning Update the Credit Authorities Addendum Update the Portfolio Review Guideline Section 7: Update to Skills Training and Accreditation Appendix C: Update to CIB Credit Risk 2LoD Process Owners Appendix D: Update to SAR 2LoD Process Owners Other minor update 	Non-Material	Christina Khoo	1.3	7 Oct 2024

The full version history is included in the RTF [Appendix G](#).

Chapter Three

1. Overview of the CIB Credit Risk Type Framework

1.1 CIB Credit Risk related principles

The Group allocates responsibilities for the Credit Risk in a manner consistent with the three **Line of Defence** (LoD) Model outlined in Part A of the ERMF. The CIB Credit RTF (this Chapter) outlines the areas of governance and risk management approach unique to the PRT.

Lending to counterparties must be subject to a robust credit assessment that includes an evaluation of the client's credit quality including willingness, ability, and capacity to pay. A suitability and appropriateness assessment needs to be completed for all counterparties to ensure only credit products / facilities which are appropriate to the nature and scale of the counterparty's business are provided.

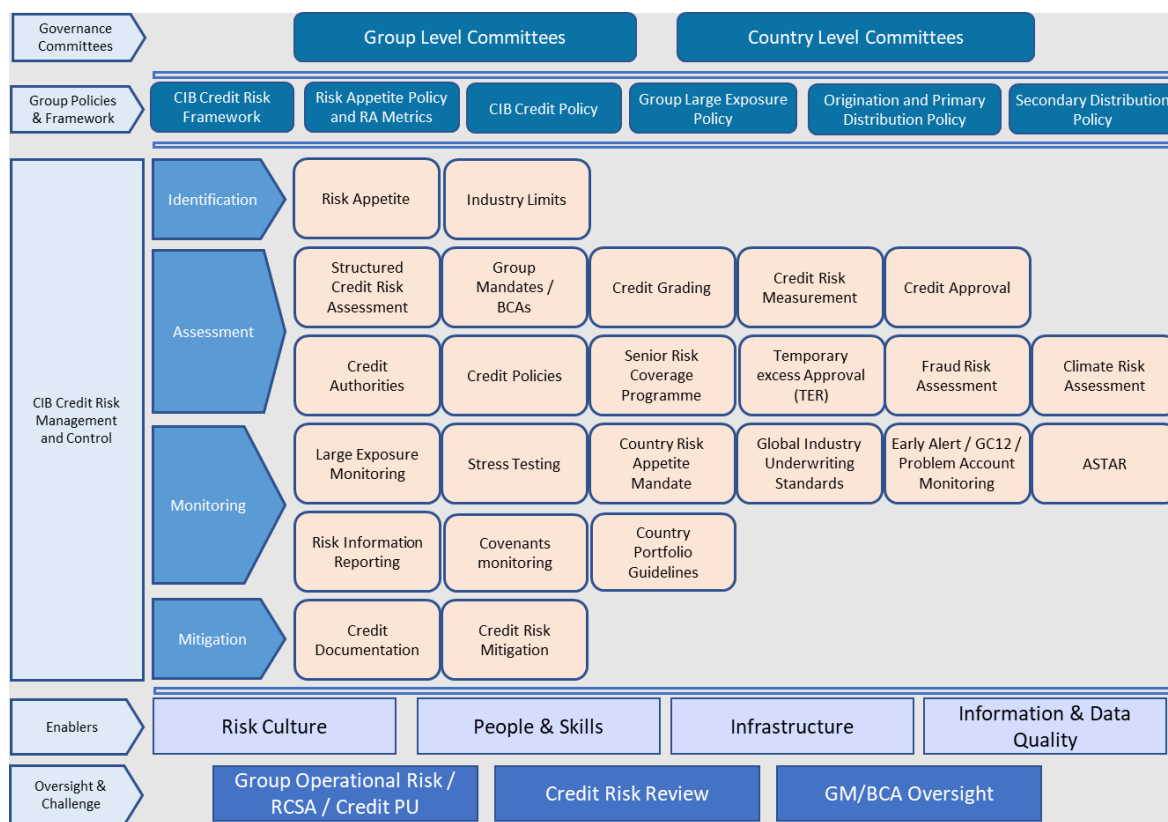
No actual, contingent, or other credit exposure may be entered into, which:

- cannot be identified, assessed, and measured.
- cannot be monitored and limited throughout the term of the exposure.
- is not capped by a maximum acceptable exposure limit and tenor.
- is prohibited by Group policy or applicable laws or regulations.
- is intended to be used for illegal or immoral purpose or where the purpose is not known,
- has not been assessed in the context of Group's sector Risk Acceptance Parameters.
- exposes the Group to material non-credit risks that have not been assessed, documented, and authorised, such as through a product programme; and
- has not been explicitly approved by an authorised individual / committee.

1.2 Overview of CIB Credit Type Framework

Figure 1 below shows the overall approach for CIB Credit Risk management.

Figure 1: CIB Credit Risk Type Framework



The Credit Risk function is the 2LoD that performs independent challenge, monitoring and oversight of the credit risk management practices of the business and functions engaged in or supporting revenue generating activities which is the first LoD.

This Chapter sets out the risk management approach, through which the Group control and optimize its risk-return profile. It is a Group-wide activity and can be grouped into four inter-dependent risk management categories as follows:

- **Identification** – Set risk appetite in line with strategic objectives. Having a clear and coherent strategy and the discipline to adhere to it is the most important foundation for the effective management of risk. There is a considered and deliberate process by which it is decided how much risk the Group want to take on, where we want to assume that risk and how we will prepare for it.
- **Assessment** – Evaluate and measure all material risks on a proactive and continual basis across by counterparty across the portfolio.
- **Monitoring** – Monitoring and control of all material risks on a proactive and continual basis by counterparty across the portfolio. Promptly identifying any clients demonstrating signs of stress and subjecting those accounts to more frequent and increased scrutiny through the Early Alert process. Problem accounts graded **Credit Grade** (CG) 13 and 14 are transferred to and managed by **Stressed Assets Group** (SAG) and **Stressed Assets Risk** (SAR).
- **Mitigation** – Ensuring all facilities extended to clients are documented and where security has been taken, that it is controlled. Facility structuring and collateral are used to further mitigate credit risk.

1.3 Updates to Credit Risk Type Framework

The **Co-Head - Chief Risk Officer** (CRO), CIB¹ or Head, Policy and Process, CIB can authorise non-material changes to this chapter.

Credit Risk Policies and Standards are approved by Head, Policy, and Process, CIB, while non-material changes to the Credit Risk Policies and Standards can be approved by Head, Credit Policy, CIB. Any dispensations/exceptions with respect to compliance of the policies/standards must be escalated to Head, Policy, and Process, CIB for review and approval.

¹ Co-Head – Chief Risk Officer (CRO), CIB refers to Co-Head-CRO, CIB and CRO, ASEAN & South Asia in this document.

2. Three Line of Defence Roles and Responsibility and Governance Committee Oversight

The Credit RTF reinforces clear accountability and roles for managing risk through the Three LoD model. The 1LoD is the Business (i.e., **Relationship Manager (RM)**² in consultation with the relevant Products³ and **Syndicate & Financing Risk (S&FR)**. CIB Credit Risk forms the primary 2LoD function with Group Internal Audit being the 3LoD. The detailed set of Global, Cluster and Country-level roles for 1LoD and 2LoD is provided in Figure 2 below:

Figure 2: Roles and Responsibilities of 1LoD and 2LoD

		Standard Chartered PLC Board					
		Board Risk Committee (BRC)					
		Group Risk Committee (GRC)					
		1LOD or Process Universe Owner (Owns and manages risk)			2LOD or RFO (Oversight and challenge)		
		Client-businesses	Products	Functions	Client-businesses	Products	Functions
Global level	Global Committee: - Group Risk Committee (GRC), - Corporate and Investment Banking Financial Risk Committee (CIBFRC) - Corporate and Investment Banking Non-Financial Risk Committee (CIBNFR) - Model Risk Committee (MRC) - Investment Committee (IC)	Co-Heads of Corporate & Investment Banking (CIB)		Global Process Owners (for credit risk processes)	Co-Head-CRO, CIB		
Executive and Cluster level	Executive Committee: - Standard Chartered Bank Executive Risk Committee (SC Bank ERC) Cluster Committees: - Africa Risk Committee (Africa RC) - Middle East and Pakistan Risk Committee (ME & Pakistan RC)	Global Head of Corporate Coverage, Global Co-Heads of Financial Institutions Coverage, Products Heads, Global Heads of S&FR, Cluster Heads of Banking & Coverage and Markets		N/A	CROs, CCOs		
Country level	Country Committee: - Executive Risk Committee (ERC) - Credit Issues Committee (CIC)	Country Heads of Banking & Coverage and Markets, Country SAG rep, Product Heads, S&FR Heads		Country Process Owners (for credit risk processes)	CROs, SCOs, Country SAR rep		
					Group Internal Audit		

Note: The Terms of Reference of the above committees are available [here](#).

The 1LoD responsibilities include:

- client on-boarding and due diligence
- credit origination including facility structuring
- credit Initiation and evaluation including **Business Credit Applications (BCA)** preparation
- monitoring and control
- co-management of certain CG12-14 accounts by CIB RM and SAG

The 2LoD (including SAR for CG13-14) is responsible for independent challenge, monitoring and oversight of the Credit Risk management practices of the first line of defence. In addition, they ensure that credit risks are properly assessed and transparent; and that credit decisions are controlled in accordance with the Group's Risk Appetite, credit policies and standards. Please refer to [Appendix B](#) of this chapter for details on 2LoD processes and process owners for CIB Credit Risk.

The 3LoD provides independent assurance of the effectiveness of controls that support 1LoD's risk management of business activities and the processes maintained by the 2LoD. Its role is defined and overseen by the Audit Committee of the Board.

² Supported by the Credit Analysts (CA) or Portfolio Analytics and Monitoring (PAM) team in accordance with the CA and PAM Roles and Responsibilities (R&R).

³ Products include Transaction Services, Banking and Markets.

3. Decision Making Authority and Delegation

The Credit RTF is the formal mechanism of delegating Credit Risk authorities cascading from the GCRO, as the Senior Manager of the Credit Risk PRT.

These individuals are delegated credit risk authorities directly via the CIB Credit Risk Type Framework and do not require separate documentation:

- **Group Chief Risk Officer** (GCRO)
- Co-Head-CRO, CIB
- **Global Head, Stress Assets Risk** (GH, SAR)

The Co-Head-CRO, CIB delegates authorities to designated individuals or Policy Owners through this Chapter, including 2LoD ownership at a global business, product, and function level as well as cluster or country level.

Credit Risk Authorities are delegated to the following roles:

Client-segment Level Credit Sanctioning	
1.	GCRO
2.	<u>Dual Sanctioning points consisting of any two of the following:</u> <ul style="list-style-type: none"> • Co-Head-CRO, CIB and CRO, ASEAN & South Asia • CRO, Americas • CRO, Africa and Middle East • Chief Credit Officer (CCO), ASEAN and South Asia & Greater China and North Asia and Global CCO (GCCO), Financial Institution Risk • GCCO, Specialised Finance Risk • CRO and CCO, Europe – for all Solo Large Exposure
3.	Co-Head-CRO, CIB and CRO, ASEAN & South Asia
4.	Global Head (GH), SAR
5.	<ul style="list-style-type: none"> • CCO, ASEAN and South Asia & Greater China and North Asia and Global CCO, Financial Institution Risk • GH, Traded Risk Management (GH, TRM) • GCCO, Specialised Finance Risk
6.	Chief Credit Officer (CCO)
7.	Senior Credit Officer (SCO)
8.	Senior Credit Manager (SCM) / Credit Manager (CM)

The Co-Head-CRO, CIB is responsible for the Credit and Investment approval authorities and Head, Policy, and Process, CIB is responsible for embedding the key requirements into the detailed client and product segment level credit policies and related standards.

Principles of Delegation of Authorities:

- Delegations do not remove the responsibilities of the delegator; and ongoing oversights are needed.
- Segregation of duties – Risk approval authority must not be delegated to individuals whose primary responsibilities relate to revenue generation. Under no circumstances, should an individual authorise charge-off and/or individual impairment provision for an account that was underwritten and approved by the same individual, except for GCRO.
- The authority recipient must have the required experience and judgement to exercise the proposed risk authorities and must either meet any applicable certification and/or experience requirements.
- Authority delegators are responsible for monitoring the quality of the risk decisions taken by their delegates and the ongoing suitability of their authorities. This is ensured through monthly oversight of approved BCAs by the credit delegator.

Risk authorities are linked to individual appointments where authorities are delegated. These individuals then in turn delegate authorities to individuals in writing in accordance with the list of delegated authority matrices and principles of delegation of authorities. Delegations vary based on business segment, limit category, CG, expected loss and maximum tenor. Details of the delegated authority matrices is included in the [Credit Authorities Addendum](#) to this Chapter.

The GCRO acts as the senior most authorised body for approving credit and covers investment / divestment approvals for aircraft, shipping, operating leases, and debt / debt like instruments (including Mezzanine and Alternate Investments), in accordance with its terms of reference in addition to corporate credits meeting specific criteria.

4. Dynamic Risk Identification

Risk identification requires a thorough analysis of the non-financial and financial risks of a client. Non-financial risks include industry, business, and management. The 1LoD carries out the primary risk identification and analysis duties with review and oversight undertaken by the 2LoD.

Continuous monitoring and control of credit exposures both individually and at a portfolio level are essential to promptly identifying any changes in situation which may lead to a deterioration in credit quality.

- At the individual client level, this requires a continuous review of the non-financial and financial risks faced by a client. Where deviations from the expected norm are anticipated, portfolio reviews are required.
- At the portfolio level, this requires constant evaluation of the economic environment both globally and at the country level, including shifts in industry conditions either due to macro-economic factors, regulatory changes, or movements in commodity prices. Portfolio reviews may be conducted at a country, cluster or global level. Refer to the [Portfolio Review Guideline](#) for detail.
- The **Credit Underwriting Principles** (CUPs) provide the credit risk principles and metrics for underwriting for Industry Portfolio Reviews.
- Stress testing should also be undertaken to assess the level of credit loss the Group may incur as a consequence of extreme but plausible events. All portfolio reviews and stress tests should include time bound action plans to right size exposures where concerns are identified.

The output of the above processes is communicated by the Co-Head-CRO, CIB and discussed at the **CIB Financial Risk Committee** (CIB FRC).

5. Regulatory Obligations and Escalation Mechanism

5.1 Group-level Regulatory Obligations

The Co-Head-CRO, CIB is responsible for ensuring 2LoD oversight and challenge of legal and regulatory risks associated with their respective areas of responsibility, as covered by the following areas of regulations:

Table 1: Areas of regulations related to CIB

Area of Law and Regulation	Subject Matter Expert
Prudential - Credit Risk Rules	Co-Head-CRO, CIB
Customer Insolvency	Co-Head-CRO, CIB

An annual attestation is conducted at Group level to facilitate periodic senior management oversight on Prudential Compliance attestation. Evidence of compliance along with resolution plan (if any) are noted for items with gaps as part of the attestation. The attestation completion is notified to Compliance and noted at CIB FRC for governance oversight.

5.2 Breach and escalation mechanism

The Co-Head-CRO, CIB is responsible for developing a breach and escalation mechanism for issues determined to be material by the RFO. Escalation of breaches should be aligned with the response management requirements set out in the [Group Operational Risk Standard](#).

6. Capital Adequacy

CIB Credit Risk is subject to minimum requirements in accordance with the UK CRR in order for the Group to operate within Risk Capacity. At Group and Solo level, Risk Capacity consists of Pillar 1 and 2A requirements.

In accordance with the overall capital adequacy rule, an ICAAP where an assessment of the Pillar 2A risks (i.e. risks that are not covered, or not sufficiently covered, by Pillar 1 is undertaken annually. The assessment forms the basis for the Regulator's **Supervisory Review and Evaluation Process (SREP)** which together with the Pillar 1 CRR minimum requirements, determines the Group's **Total Capital Requirement (TCR)**. Firms are expected to maintain financial resources at or above the level specified in the TCR at all times.

The Co-Head-CRO, CIB is responsible for defining appropriate scenarios, ensuring the outcomes are reflective of the residual risks in their areas and can determine if any additional Pillar 2A add-on is needed based on any material residual risks.

At a Group and Solo level, the Pillar 2 assessment for CIB Credit Risk is managed by Co-Head-CRO, CIB. Local regulators may have an approach that may vary slightly, in such cases local regulations should prevail.

7. Skills Training and Accreditation

The 1LoD and 2LoD in CIB must have the technical skills and knowledge to discharge their responsibilities in relation to credit risk management diligently and effectively.

The **Core Credit Curriculum (CCC)** certifications are designed to provide a consistent level of skills-based training to enable rigorous and forward-looking credit assessments and credit decision making. For employees who propose, support, or approve **Group Mandates (GMs)/BCAs**, they are required to have CCC certification which comprises at least one of the following certifications:

- **Client Management Credit Curriculum (CMCC)**
- **Corporate Credit Risk Management Certification (CCRMC).**
- **Financial Institutions Risk Certification (FIRC)**
- **CCC Senior Manager Understanding (CCC-SMU)**

The employees need to register for these certifications within 12-months of moving into an affected role, and complete within 12 months upon registration. This is a job requirement for all employees who propose, support, or approve BCAs/GMs.

There are other CCC courses, which are aimed to support the employees with the Group's credit management framework but not a requirement for employees who propose, support, or approve GMs/BCAs

Please refer to [Governance Handbook](#) for all CCC programmes.

Appendices specific to this Framework

Appendix A - Credit Risk references to Climate Risk, Digital Asset Risk and Third-Party Management Risk

Credit Risk is also exposed to certain risks which are significant in nature as follow:

Risk	Cross Reference Context
Climate	<p>Climate Risk is the potential for financial loss and non-financial detriments arising from climate change and society's response to it. This manifests in Credit Risk through the financial impact of physical risk and transition risk to our clients. This refers to:</p> <ul style="list-style-type: none"> ▪ Transition risk – sustained decrease in revenue due to reduced market demand for higher carbon products/ commodities; increase in costs resulting from premature write-downs or stranded assets; increase in capital expenditure related to climate risk adaptation or rise in expenses due to rising carbon tax ▪ Physical risk – the potential for increased capital and operating expenditure driven by impact of acute weather risk, such as asset damage, repair costs and business interruption; or stress on natural resources (e.g. water stress)
Digital Asset	<p>Digital Asset Risk is the potential for regulatory penalties, financial loss and or reputational damage to the Group resulting from digital asset exposure or digital asset related activities arising from the Group's Clients, Products and Projects. This manifests in Credit Risk through credit relationships with Crypto asset Service Providers (CASPs) which are defined as:</p> <ul style="list-style-type: none"> ▪ Crypto asset Exchange Providers – entities which exchange or make arrangements to exchange crypto assets for fiat currency, other crypto assets, operates machinery that facilitates such exchanges, or issue of crypto assets (including Initial Coin Offerings or Initial Exchange Offerings) ▪ Crypto asset Custodian Wallet Providers – which provides business services to safeguard crypto assets on behalf of its customers, holding private cryptographic keys on behalf of customers to hold, store and transfer crypto assets <p>Digital Asset risk may also emerge through non-CASP relationships where such an entity uses crypto assets in terms of revenue or business model or provides supporting services to CASP entities (e.g. crypto asset mining firms).</p>
Third Party Risk Mismanagement	Potential for loss or adverse impact due to the failure to manage the onboarding, lifecycle and exit strategy of a third party.

Appendix B - CIB Credit Risk 2LoD processes

Processes	Definition
Credit Approval	The review, challenge, and approval of requests for credit limits for clients based on the credit risk analysis submitted by the credit analysts and relationship managers as the 1LoD.
Fulfilment	The completion of documentation formalities for credit limits approved. This includes the checking of security documents, security perfection and maintaining custody of all facility documentation and limit activation.
Monitoring including Collateral	The ongoing monitoring of facilities including daily excesses and past dues, covenants and overdue and extended Group Mandates and BCAs. Collateral monitoring covers completion of documentation and, where appropriate, the related security matters and dated facility and security documents,
EAR / ASTAR	The monitoring of all accounts on EA and ASTAR and completing facility documentation checks for all accounts when initially placed on ASTAR.
Policy Formulation and Implementation	Review, and approval of CIB policies and procedures. Communication and implementation of updated policies and procedures for CIB
Risk Reporting	Credit Bureau and country regulatory reporting.

Appendix C - CIB Credit Risk 2LoD process owners

Risk Name / ID	Process Name	Group PO	Group RFO
Process governance\ RISK-00078587	Credit Approval - Delegation of Credit Authority	Head Credit Policy CIB	Head, Policy and Process, CIB
Process governance\ RISK-00078585	Credit Approval - Credit Authority Review	Head Credit Policy CIB	Head, Policy and Process, CIB
Process governance\ RISK-00077630	Credit Approval - BCA, Temporary Excess (non-FM) and DDW Approval	Head Credit Policy CIB	Head, Policy and Process, CIB
Process governance\ RISK-00077632	Credit Approval - Risk Appetite (Counterparty Level)	Head Credit Policy CIB	Head, CFCC Advisory, Functions
Process governance\ RISK-00075241	Credit Early Alert/ASTAR - ASTAR Monitoring	Head Credit Policy CIB	Head, Policy and Process, CIB
Process governance\ RISK-00078589	Credit Monitoring - Risk Appetite and Portfolio Guidelines Monitoring	Head Credit Policy CIB	Head, Policy and Process, CIB

INTERNAL

Risk Name / ID	Process Name	Group PO	Group RFO
Process governance\ RISK-00086267	Credit Monitoring - Credit Documentation Check	Head Credit Policy CIB	Head, Policy and Process, CIB
Process governance\ RISK-00077983	Credit Regulatory Check - Review, Approval and Implementation of Credit Policies & Standards	Head Credit Policy CIB	Head, Policy and Process, CIB
Regulatory adherence\ RISK-00086049	Credit Concentration Risk - Large Exposures (LE) Monitoring	Head Credit Policy CIB	Head, Policy and Process, CIB
Regulatory adherence\ RISK-00077480	Credit Monitoring - BCA Renewals and Extensions	Head Credit Policy CIB	Head, Policy and Process, CIB
Regulatory adherence\ RISK-0000002928	Credit Monitoring- Portfolio Review	Senior Manager Governance	Head, Industries Risk
Regulatory adherence\ RISK-00077631	Credit Monitoring – CG12 and Early Alert Reporting and Monitoring	Head Credit Policy CIB	Head, Policy and Process, CIB
Regulatory adherence\ RISK-00078586	Credit Monitoring - Daily Excess and Past Dues Monitoring (non-FM)	Head Credit Policy CIB	Head, Policy and Process, CIB
Governance of Regulatory Adherence\ RISK-0000002019	Credit Regulatory Check - ICAAP Pillar 2A Credit Risk Assessment	Head Credit Policy CIB	Head, Policy and Process, CIB
Non-public information\ RISK-00086456	Risk Reporting - Misuse of Information - Governance Committee – IC	Head Credit Policy CIB	Executive Director, CFCC CIB Client Coverage
Credit fraud\ RISK-00086268	Credit Approval - Credit Fraud	Head Credit Policy CIB	Executive Director, CFCC CIB Client Coverage
Data quality\ RISK-00087470	Credit Monitoring - Data Quality	Head Credit Policy CIB	Director, CFCC Data Conduct - Data Quality
Regulatory adherence\ RISK-00080802	BCA Preparation Review and Extension, Credit Grading and Financial Analysis	Head, Process & Governance	Head, Policy and Process, CIB

INTERNAL

Risk Name / ID	Process Name	Group PO	Group RFO
Regulatory adherence RISK-0000002561	Climate Risk BCA Integration	Head, Process & Governance	Head, Policy and Process, CIB
Regulatory adherence RISK-00078287	Excess & Past Due Management	Head, Process & Governance	Head, Policy and Process, CIB
Regulatory adherence RISK-00078442	Early Alert Reporting and Management of CC owned CG12/13/14	Head, Process & Governance	Head, Policy and Process, CIB
Process governance RISK-00084936	Intragroup Limit Allocation (ILA)	Head, Process & Governance	MD, Treasury CRO, Europe & Americas
Process governance RISK-00086243	EL Computation	Head, Process & Governance	Head, Policy and Process, CIB
Process governance RISK-00078801	CaRT Monitoring & Document Deferral Management	Head, Process & Governance	Head, Policy and Process, CIB
Process governance RISK-00086242	ASTAR Monitoring	Head, Process & Governance	Head, Policy and Process, CIB
Credit fraud RISK-00076653	External Fraud	Head, Process & Governance	ED, CFCC CIB Client Coverage
Misselling RISK-00078774	Client Conduct - Mis selling	Head, Process & Governance	ED, CFCC CIB Client Coverage
ESG execution RISK-00080803	Reputational and Sustainability Risk Materiality Assessment (RSRMA) & Environmental and Social Risk Assessment (ESRA)	Head, Process & Governance	Global Head, Climate, Sustainability & Reputational Risk
Greenwashing RISK-0000003243	Greenwashing	Head, Process & Governance	Global Head, Climate, Sustainability & Reputational Risk
Process Governance RISK-00080868	Collateral Maintenance	Head, Process & Governance	Head, Policy and Process, CIB

INTERNAL

Risk Name / ID	Process Name	Group PO	Group RFO
Process Governance RISK-00078778	Collateral and Documentation Expiry Monitoring & Early Alert Documentation Check	Head, Process & Governance	Head, Policy and Process, CIB
Process governance RISK-00086782	Credit Static Data	Head, Process & Governance	Head, Policy and Process, CIB
Process governance RISK-00078748	Limit Activation & Maintenance	Head, Process & Governance	Head, Policy and Process, CIB
Transaction execution RISK-0000002684	Audit Confirmation & Balance Confirmation	Head, Process & Governance	ED, OTCR, CIB
Record Keeping RISK-00076142	Custody of Credit and Security Documents	Head, Process & Governance	Head, Policy and Process, CIB
Non financial regulatory reports RISK-00084980	Country Regulatory Reporting	Head, Process & Governance	ED, CFCC CIB Client Coverage
Non-Financial Regulatory Reports RISK-00077637	Credit Bureau Reporting & Single Borrower Limit (SBL) Monitoring	Head, Process & Governance	Head, Policy and Process, CIB
Legal enforceability RISK-00085021	Global Template Management	Head, Process & Governance	Head, Legal, Client Coverage, CIB
Credit Fraud - RISK-00080860 Legal Enforceability - RISK-00080862 Process Governance-RISK-00080868	Credit Fraud/Legal Enforceability/Process Governance - Credit Documentation - CRC	Head, Process & Governance	ED, CFCC CIB Client Coverage / Head, Policy and Process, CIB / Head, Policy and Process, CIB

Appendix D - SAR 2LoD process owners

Risk Name / ID	Process Name	Process Definition	GPO	GRFO
Credit Approval -BCA / RFA Approval - [Process governance]\RISK-0000002293]	Credit Approval (PROC-00035604)	The approval of Request for Action in relation to account strategy and major actions taken on the CG13-CG14 account and engagement of 3rd party professionals	Head, Policy and Process, CIB	Global Head, Stressed Assets Risk

INTERNAL

Risk Name / ID	Process Name	Process Definition	GPO	GRFO
Credit Approval – Delegation of Authority [Process governance\RISK-0000002662]	Credit Approval (PROC-00035604)	The approval of Request for Action in relation to account strategy and major actions taken on the CG13-CG14 account and engagement of 3rd party professionals	Head, Policy and Process, CIB	Global Head, Stressed Assets Risk
Credit Monitoring -Daily Excess Monitoring - [Regulatory adherence\RISK-0000002294]	Monitoring including Collateral (PROC-00035637)	The monitoring of 90 days past due for the identification of default. The ongoing monitoring of credit grade and daily excess (including placement of liens/risk markers), collateral valuation and compliance with Transactional Conflicts & Information Wall Procedures.	Head, Policy and Process, CIB	Global Head, Stressed Assets Risk
Credit Monitoring – SARR Monitoring [Process Governance\RISK-0000002661]	Monitoring including Collateral (PROC-00035637)	The monitoring of 90 days past due for the identification of default. The ongoing monitoring of credit grade and daily excess (including placement of liens/risk markers), collateral valuation and compliance with Transactional Conflicts & Information Wall Procedures.	Head, Policy and Process, CIB	Global Head, Stressed Assets Risk
Regulatory Risk – CLP [Process governance\RISK-0000002296]	Credit Loss Provision	The IFRS 9 assessment by account managers and approval by officers with Delegated Authorities of Stage 3 individual impairment submitted in the Individual Impairment Report and the raising of journal entries.	Head, Policy and Process, CIB	Global Head, Stressed Assets Risk
Regulatory Risk – PAMS [Process governance\RISK-0000002295]	Policy Formulation & Implementation (PROC-00035917)	Problem Accounts includes all non-performing exposures in the banking book in CIB and any other exposures, including exit portfolio(s)	Head, Policy and Process, CIB	Global Head, Stressed Assets Risk

Appendix E - Credit Risk references to other RTFs

Cross Reference Context	
Operational & Technology Risk	For assessing effectiveness of the control system, this RTF refers to the Operational and Technology RTF and Risk and Control Self-Assessment (RCSA) which sets out a consistent approach to control design specification, operating effectiveness of the controls, and rating. All risk assessments and risk event responses are to be guided by Group Operational Risk Policy and Standards and managed through the infrastructure set out by the Operational and Technology Risk function.
Environmental, Social and Governance and Reputational Risk (ESGR)	This RTF refers to the ESGR RTF that sets out how 1) reputational risks, including stakeholder perception risks and greenwashing risks, arising from the failure or non-compliance of CIB Credit Risk; 2) environmental (including climate) and social risks should be identified, assessed and managed. Such consequential reputational and ESG risks if material, should be notified to the Risk Framework Owner for ESGR.
Compliance Risk	For areas of regulations related to CIB Credit Risk, the Co-Head-CRO, CIB must ensure that all responsibilities of the 2LoD as specified in section 5 of the ERMF are carried out in addition to the specific requirements on regulatory obligations as set out in Section 5 of this RTF.
Traded Risk	Market risk events e.g., movements in FX, interest rates and commodity prices leading to credit risk migration at the counterparty level
Financial Crime Risk	Financial Crime Risk events impacting a counterparty's ability to repay / service debt
Information and Cyber Security Risk	A malicious account data leak / theft could reduce the client's ability to repay
Treasury Risk	Lack of access to functioning capital and liquidity markets could impair the ability of clients to repay particularly where the counterparty is exposed to refinancing risk.
Model Risk	Effective management of Credit Risk models

Appendix F - Risk Reporting

All **Critical Risk Measures** (CRM) and **Critical Data elements** (CDE) along with their definitions are available in Axon ([link](#)). Any changes to the definitions of CRMs/CDEs will need to be done by the respective reporting teams, post approval from Group RFO / Board.

Appendix G – Version Control

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Zeeshan Arif	Initial version created as part of the consolidation of standalone RTFs during the ERMF/RTF simplification exercise.	Material	SC PLC Board	1.0	7 Dec 2023
Zeeshan Arif & Ankit Sanklecha	Part B - Credit RTF(CCIB) <ul style="list-style-type: none"> Global Credit Markets (GCM) Head has been added in the 1LoD R&R - (GCM) now report into both Financial Markets (FM) and Client Coverage (CC). 	Non-Material	Christina Khoo	1.1	05 Jan 2024
Renzo Baio	CIB Credit RTF. <ul style="list-style-type: none"> Update to reflect the change from CCIB to CIB Update to Figure.2 on the Roles and Responsibilities of 1LoD and 2LoD to include Cluster Heads of businesses and S&FR. Section 3: Updates to Client-segment credit sanctioning authorities ERMF Part C: <ul style="list-style-type: none"> Included Origination and Distribution policy under CIB Credit. Updates to reflect changes from CCIB to CIB in appendices. 	Non-Material	Christina Khoo	1.2	31 May 2024
Oki Darvian	Part B – CIB Credit RTF. <ul style="list-style-type: none"> Amend 'CRO, CIB' title to 'Co-Head – CRO, CIB' Figure 2: Update to the Banks committee names Section 3: <ul style="list-style-type: none"> Update to Client-segment Level Credit Sanctioning Update the Credit Authorities Addendum Update the Portfolio Review Guideline Section 7: Update to Skills Training and Accreditation Appendix C: Update to CIB Credit Risk 2LoD Process Owners Appendix D: Update to SAR 2LoD Process Owners Other minor update 	Non-Material	Christina Khoo	1.3	7 Oct 2024

Note: Please refer to part C of ERMF for common Appendices.

----- END OF CHAPTER THREE -----

WRB CREDIT RISK TYPE FRAMEWORK

Chapter Number	Four – Part B of the ERMF
Principal Risk Type	Credit Risk – WRB
Risk Framework Owner Name	Xiaomin Rong
Risk Framework Owner Job Title	CRO, WRB
Document Contact Name	Khurram Awais Siddique
Document Contact Job Title	Global Head, Policy & Governance
Version Number	1.2

Contents

1. Overview of the WRB Risk Type Framework..... 3

1.1. WRB Credit Risk management principles..... 3

1.2. Overview of WRB Credit Risk Type Framework 3

2. Three Lines of Defence Roles and Responsibilities 4

3. Governance Framework and Governance Committee Oversight 5

3.1. Decision Making Authority and Delegation 5

3.2. Governance Committee Oversight at Group, Regional and Country level 5

4. Regulatory Obligations and Escalation Mechanism 7

4.1. Group-level Regulatory Obligations 7

4.2. Country-level Regulatory Obligations 7

4.3. Breach and escalation mechanism 7

Appendices specific to this Framework..... 8

Appendix A: Credit Authorities Addendum – WRB..... 8

Appendix B: Version Control..... 8

Version Control Table

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Dipti Bhatia	Minor updates to align with changes to terminology, such as 'country' to 'market', Committee names etc.: 1) Figure 1: Included Higher Risk Markets Forum within Mitigation tab. 2) Committee names have been updated on page 7 and 8 in line with the existing terminologies.	Non-material	Xiaomin Rong	1.2	09 Dec 2024

The full version history is included in the RTF [Appendix B](#).

Chapter Four

1. Overview of the WRB Risk Type Framework

The WRB Credit RTF (this Chapter) outlines the areas of governance and risk management approach unique to the PRT.

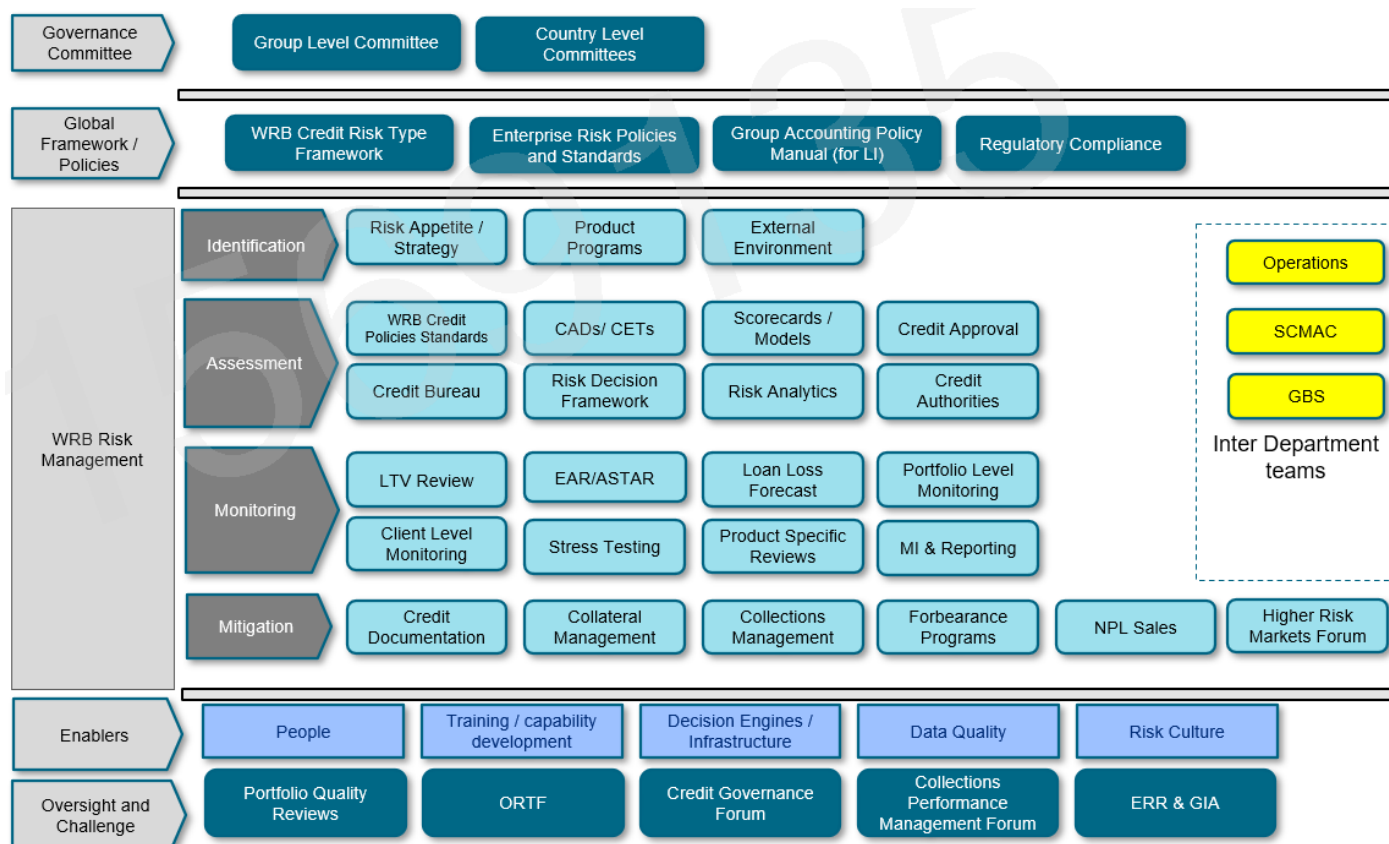
1.1. WRB Credit Risk management principles

- All credit risk assumed must be within the Group's Risk Appetite and consistent with the approved strategy.
- Credit Exposures will be permitted only against products / facilities which are at minimum covered by an approved **Product Program Guide (PPG)/ Credit Risk Management Policy (CRMP)/ Credit Approval Document (CAD)** and **Credit Expansion Testing Document (CET)**.
- All Credit exposures booked must be measured, monitored, recorded and capped. The maximum acceptable exposure limit and tenor with details of collateral information must be recorded.
- Lending decisions are based primarily on repayment capability¹. A holistic approach is adopted in assessing the client's needs by assessing income, risk profile & indebtedness to determine their ability and willingness to service total debt.
- As outlined in Part A of the ERMF the RFO has the authority to make non-material changes to this Chapter. Within WRB, non-material changes comprise of administrative changes (for example, updating links, updating designations due to an organizational change). For the avoidance of doubt, all substantive changes to the principles articulated in this chapter are considered material.

1.2. Overview of WRB Credit Risk Type Framework

Figure 1 below shows the overall approach for WRB Credit Risk management at the Group.

Figure 1: Overview of WRB Credit Risk Management



¹ Collateral based lending is allowed in specific products. Collateral based lending is when the credit decision is based mainly on the collateral and not on the repayment capability.

In WRB, credit risk is managed based on the rule-based (or programme) and discretionary approach (for Wealth Management Private Banking and Business Banking Medium Enterprise segment). However, the core principles of risk management remain the same in both approaches.

This Chapter is grouped into four inter-dependent risk management phases based on Credit Risk life cycle, as follows:

- **Identification:** Set Risk Appetite in line with strategic objectives. Having a clear and coherent strategy and the discipline to adhere to it is important for effective management of risk. This is a measured process by which it is decided how much risk the Group wants to take on, where the Group wants to assume that risk and how the Group will prepare for it.
- **Assessment:** Evaluate and measure all material risks on a proactive and continuous basis at counterparty and portfolio level.
- **Mitigation:** Ensuring all facilities extended to clients are documented and where collateral has been taken, it is controlled and legally enforceable. Collateral Enforcement and Forbearance Measures are used to further mitigate credit risk.
- **Monitoring:** Monitoring and control of all material risks on a proactive and continuous basis at portfolio level and/or at counterparty level across different client segments. Promptly identifying any clients or segment demonstrating signs of stress and apply necessary portfolio management and collection measures. Stress tests are regularly performed to assess resilience to extreme but plausible market conditions.

Business acquired through portfolio acquisitions and partnerships may have a separate execution approach based on the transaction structure of such deals approved by the delegated authority.

2. Three Lines of Defence Roles and Responsibilities

The WRB Credit RTF reinforces clear accountability and roles for managing risk through the LoD model. The 1LoD is the business and functions engaged in or supporting revenue-generating activities. Risk forms the primary 2LoD of defence function. The detailed set of global, regional/cluster and market/local level roles and responsibilities for the 1LoD and 2LoD are provided in Figure 2 below.

Figure 2: WRB Credit Risk - Overview of the Three LoD

Standard Chartered PLC (Board)			
Board Risk Committee (BRC)			
Group Risk Committee (GRC)			
Wealth & Retail Banking Risk Committee (WRBRC)			
	1LoD or Process Universe Owner (owns and manages) risk)	2LoD or RFO (oversight and challenge)	Third LoD (independent assurance)
Global	CEO, WRB supported by Global Business Heads	CRO, WRB supported by Global Product/Function Risk Heads	Group Internal Audit
Regional / Cluster	Regional or Cluster Heads, WRB	Chief Credit Officers, WRB supported by Country Credit Heads (CCH)	
Market /Local	Country Heads, WRB supported by Business Heads	Country Credit Head, WRB supported by Country Product/Function Risk Heads	

At the market/local, regional and global levels, the respective CEOs and Business Heads are the 1LoD of WRB credit risk. The 1LoD must comply with the applicable laws, regulations and regulatory expectations and manages the risk that arises from 1LoD activities. The 1LoD is further accountable for embedding the credit risk management approach set by CRO, WRB.

The 1LoD responsibilities include:

- client value proposition and product management
- propose credit proposals with regard to risk-reward balance
- channel, sales management and client communication
- credit initiation and evaluation within credit policies and standards
- client on-boarding, documentation and due diligence
- transaction processing and payment
- monitoring and control
- co-management of certain problem accounts

The 2LoD provides an independent challenge and oversight of all credit risk taking activities and approves credit risk exposures based on delegated credit authorities. This includes the **Enterprise Risk Review (ERR)** team that independently reviews the WRB credit portfolio.

Group Internal Audit acts as the third LoD, as outlined in Part A of the ERMF.

3. Governance Framework and Governance Committee Oversight

3.1. Decision Making Authority and Delegation

This RTF is the formal mechanism through which the GCRO delegates to the CRO, WRB. The WRB Credit Risk authorities as detailed in the **Credit Authorities Addendum** under [Appendix A](#). The CRO, WRB may further delegate these authorities to credit officers with clear specifications on whether sub-delegation is allowed.

Principles of Delegation of Authorities:

- Credit Authorities are delegated solely based on personal merit, experience and capabilities to exercise the proposed delegated authorities and where applicable, should meet any qualification requirements.
- Delegations do not remove the responsibilities of the delegator, and ongoing oversight is required.
- Segregation of duties must be adhered to and risk approval authority must not be delegated to individuals whose primary responsibilities relate to revenue generation².
- Under no circumstances, should an individual authorise charge-off or individual impairment provision for an account that was underwritten and approved by the same individual, except for the GCRO³.
- Authority delegators are responsible for monitoring the quality of the credit decisions taken by their delegates and the ongoing suitability of their authorities. This can be ensured by the periodic review of the performance of approval authorities in accordance with the WRB Credit Risk Management Policy.

3.2. Governance Committee Oversight at Group, Regional and Country level

A clear hierarchy of committee responsibilities governs the Group's approach to managing WRB Credit Risk. A full overview of global, hub, regional and market level governance committees that provide primary oversight for WRB Credit Risk are shown in the table below:

² This excludes reasonable and controlled instances where delegation may be extended to a) Branch and Relationship Managers for approving temporary overdrafts/cheque purchase or for technical excesses and b) authorities granted with respect to Sand Box programs for testing booking volumes, limited to a defined number of accounts, before formally proposing CET (test program) and c) Level 1 and Level 3 authorities (defined in the WRB Credit Risk Management Policy) delegated to Credit Initiations or Collections & Recoveries teams in the 1LoD under the WRB COO. These delegations are given under controlled conditions and subject to 2LoD oversight, as defined in the WRB Credit Risk Management Policy.

³ This requirement does not apply to Medium Enterprise Problem Accounts, discounts/waivers given to customers under settlements, debt relief programs and disputed cases. The rule-based impairment as defined in Group Accounting Policy Manual does not require separate approval from any authority.

Table 1: Governance Committee Oversight

Level	Committees	Purpose
Global	GRC	The Group Risk Committee (GRC) oversees the effective implementation of the Enterprise Risk Management Framework as well as the risk management of all the Principal Risks (excluding Capital and Liquidity Principal Risk Type and Financial Crime Principal Risk Type).
	SC Bank ERC	The SC Bank ERC oversees the effective implementation of the SC Bank Risk Management Framework as well as the risk management of all the Principal Risks (excluding Capital and Liquidity Principal Risk Type and Financial Crime Principal Risk Type).
	WRBRC	The Wealth & Retail Banking Risk Committee (WRBRC) is appointed by and receives its authority from the GRC, to act as the primary senior management committee to ensure the effective management of risk throughout WRB in support of the Group's strategy.
	MRC	The Model Risk Committee (MRC) is constituted by the GRC to approve the Group model's RA and to approve model for use within the Group.
	CMAC	The Credit Model Assessment Committee (CMAC) is constituted by MRC to approve and provide oversight on Credit Risk models. These include Internal Rating Based credit risk models, models for International Financial Reporting Standards 9, stress testing models and credit scorecards.
	IFRS9 Impairment Committee	The IFRS9 Impairment Committee (IIC) ensures effective management of the Expected Credit Loss computation as well as stage allocation of financial assets for quarterly financial reporting within the authorities set by the GRC.
	CMRC	The Climate Risk Management Committee (CMRC) ensures oversight over the Group's Climate Risk workplan and embedding of Climate Risk and Net Zero targets across its businesses, as part of the Group's commitment to management of Climate Risk-related financial and non-financial risks.
	DRC	The Digital Asset Risk Committee (DRC) oversees the risk management of Digital Assets (DA) under the ERMF within WRB Businesses are required to consult the DRC for a decision from a DA Risk perspective prior to presentation in business-as-usual (BAU) committees (such as WRBRC).
Cluster	HK & GCNA RC ME & Pakistan RC Africa RC	Hong Kong & GCNA Risk Committee (HK & GCNA RC), Middle East and Pakistan Risk Committee (MEPRC) and Africa Risk Committee (ARC) are the authorised bodies for managing all risks including effective implementation of the ERMF and Principal Risk Type Frameworks (except Capital and Liquidity for the respective consolidated entities) arising from the Group's activities in the Region. These committees are appointed by GRC. HK & GCNA RC provide risk oversight of SCB Hong Kong for the purpose of local regulatory expectations. Regional risk oversight of Europe is with the UK and Europe Risk Committee.

Level	Committees	Purpose
Market/Local	ERC/CRC	Known in a subsidiary as the Executive Risk Committee (ERC) and in a branch as the Country Risk Committee (CRC). The ERC/CRC ensures the effective management of risk throughout the country in support of business strategy. The ERC/CRC ensures that risks within the country are managed effectively within the constraints set by the Group level risk committees.
	PQRF and CIC	For WRB credit portfolios the Portfolio Quarterly Review Forum (PQRF) for Group oversight is held periodically (and in some cases incorporated into the CIC) in accordance with WRB Credit Policy. The Credit Issues Committee (CIC) ensures credit issues and adverse trend in the WRB lending portfolio are identified and addressed through appropriate actions. The CIC also monitors the CIB portfolio, including oversight of Early Alert and Group Special Assets Management.

4. Regulatory Obligations and Escalation Mechanism

4.1. Group-level Regulatory Obligations

The CRO, WRB (or delegate) is responsible for ensuring 2LoD oversight and challenge of risk of non-compliance with regulatory obligations associated with their respective areas of responsibility, as covered by the following areas of regulations:

Table 2: Areas of regulation related to WRB Credit Risk

Area of regulation	Definition
Prudential – Credit Risk	The risk of failure to comply with Prudential regulations where the underlying risk is credit risk
Customer Insolvency	The risk of failure to comply with applicable Customer Insolvency management and reporting laws and regulations.

For credit related regulations issued by Financial Services Regulators (UK regulator), CFCC will identify new and amended regulations as and when issued and communicate the relevant regulatory obligations to the applicable RFO delegate.

4.2. Country-level Regulatory Obligations

The RFO (or delegate) for Credit Risk i.e., CRO, WRB (or delegate) is responsible to ensure timely implementation and compliance with credit risk related regulations. The CCH is responsible for the Local RFO activities as set out in Table 2 (above) at market/local level.

4.3. Breach and escalation mechanism

The CRO, WRB is responsible for ensuring an effective breach and escalation mechanism for issues determined to be material by the RFO.

- Market-level regulatory breaches must be escalated to the respective Chief Credit Officer, CCH, Local Compliance and Local CRO and will be discussed at the appropriate Country or Executive Risk Committee.
- Material local breaches and regulatory breaches related to Group-level regulations must be escalated to the CRO, WRB, Group Compliance and notified to WRBRC.

Appendices specific to this Framework

Appendix A: Credit Authorities Addendum – WRB

Link: [Credit Authorities Addendum – WRB](#)

Appendix B: Version Control

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Zeeshan Arif	Initial version created as part of the consolidation of standalone RTFs during the ERMF/RTF simplification exercise.	Material	SC PLC Board	1.0	7 Dec 2023
Renzo Baio	Minor updates to align with changes to terminology, such as 'country' to market or local and CPBB to WRB. Part C: <ul style="list-style-type: none">C1 & C2 Appendix: Updates to reflect nomenclature changes from CPBB to WRBC3 Appendix: Consolidation of Priority reports	Non-Material	RFO	1.1	30 Apr 2024
Dipti Bhatia	Minor updates to align with changes to terminology, such as 'country' to 'market', Committee names etc.: 1) Figure 1: Included Higher Risk Markets Forum within Mitigation tab. 2) Committee names have been updated on page 7 and 8 in line with the existing terminologies.	Non-material	Xiaomin Rong	1.2	09 Dec 2024

Note: Please refer to part C of ERMF for common Appendices.

----- END OF CHAPTER FOUR -----

TRADED RISK TYPE FRAMEWORK

Chapter Number	Five – Part B of the ERMF
Principal Risk Type	Traded Risk
Risk Framework Owner Name	Morgan Poquet
Risk Framework Owner Job Title	Global Head, Traded Risk Management
Document Contact Name	Sylvia Menezes
Document Contact Job Title	Sr. Manager, Traded Risk Regulatory Affairs & Governance
Version Number	2.0

Contents

1. Overview of the Traded Risk Type Framework 3

1.1 Traded Risk management principles3

1.2 Applicability3

1.3 Risk Management Approach for Traded Risk3

2. Three Line of Defence Roles and Responsibilities 4

3. Decision Making Authority and Delegation 4

4. Regulatory Obligations and Escalation Mechanism 5

4.1 Group-level Regulatory Obligations5

5. Group Regulatory Interpretations 5

6. Breach and escalation mechanism 6

Appendices Specific to this Framework 7

Appendix A: Traded Risk 2LoD Processes 7

Appendix B: Version Control 8

Version Control Table

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Sylvia Menezes	<p>Section 1.2: Re-introducing essential scope definition under Applicability.</p> <p>Section 2: To align oversight and management of Risk with the Group organisation design, “Hubs/ Regions” have been changed to “Clusters”.</p> <p>Section 3: Clarified Delegation of Traded Authority for Band 7 individuals.</p> <p>Added a sentence to ensure monitoring in place by RFOs for appropriate use of DCA and DTAs.</p> <p>Added a sentence to provide for instances where a country Board / ERC has an obligation to provide an independent DTA to a country risk manager.</p> <p>Section 4.1: With the transfer of Automated Trading Policy to Compliance, the reference to MIFID II RTS 6 under Table 3 has been removed.</p> <p>ERMF Part C: Transfer of Automated Trading policy to Compliance.</p>	Material	Sadia Ricke	2.0	13 Dec 2024

The full version history is included in the RTF [Appendix B](#).

Chapter Five

1. Overview of the Traded Risk Type Framework (TRTF)

1.1 Traded Risk management principles

The Traded RTF (this Chapter) outlines the governance and risk management approach unique to Traded Risk.

- Traded Risk exposures should be managed in a commercial, proportionate and risk-based manner, aligned with the Risk Appetite required to support Group strategy.
- The 1LoD and **Traded Risk Management (TRM)** as the 2LoD should use common models and infrastructure in order to establish a unique view of risk.
- The management of Traded Risk should be carried out by competent individuals with adequate model, business and product knowledge, and resourced at a level that is commensurate with 1LoD activities.

1.2 Applicability

1.2.1 Market Risk

This Framework is applicable to all businesses of the Group generating market risk either in the Trading Book or in the Non-Trading Book for which the accounting treatment is fair-valued.

1.2.2 Counterparty Credit Risk (CCR)

This Framework is applicable to all CIB clients and all financial market products undertaken by CIB, Treasury or other divisions of the Group, including Derivatives, Long Settlement Transactions, and Securities Financing Transactions, as defined in the CCR Standard.

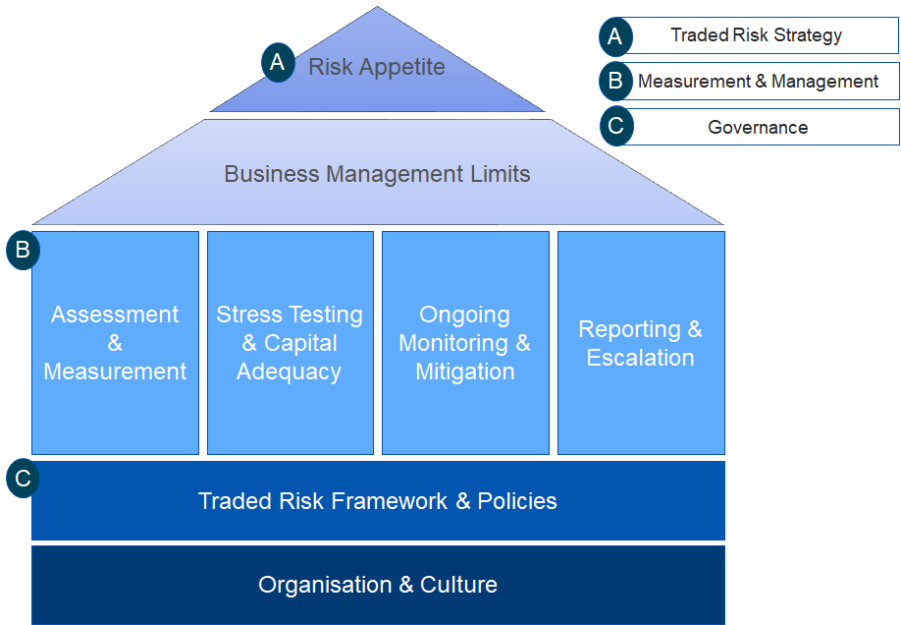
1.2.3 Other Areas of Risk

TRM should factor in risk assessment and manage considerations of Climate Risk, Third Party Risk and Digital Asset Risk. At an operating level, any additional special treatment is detailed in the Market Risk Standard and CCR Standard.

1.3 Risk Management Approach for Traded Risk

Figure 1 below shows the overall approach for TRM.

Table 1: Overall approach to TRM



2. Three Line of Defence Roles and Responsibilities

The TRTF reinforces clear accountability and roles for managing risk through the Three LoD model as outlined in Part A of the ERMF. The 1LoD is the business. TRM forms the primary 2LoD function with Audit being the third line. An overview of the model employed is shown in Figure 2 below.

Table 2: Traded Risk – Overview of the Three Lines of Defence

Global		Standard Chartered PLC Board						
		Board Risk Committee (BRC)						
	Committees: GRC, SC Bank ERC, CIB FRC, GNFRFC, FM NFRFC, MRC, VBC, GALCO, TMAC	Group Risk Committee (GRC)						
		1LoD or Process Universe Owner (owns and manages risk)			2LoD or RFO (oversight and challenge)			3LoD (independent assurance)
		Client- businesses	Products	Functions	Client- businesses	Products	Functions	
Clusters		Committees: HK & GCNA RC, SG & ASEAN RC, IN & South Asia RC, UK & Europe RC, US & Americas RC, Africa RC, ME & Pakistan RC	Global Head, CIB Global Head, Treasury Global Head, SAR Global Head, WRB	CIB COO Treasury COO	Global Head TRM	ERM OR PC VC Finance	Group Internal Audit	
Country	Committees: ERC/CRC	Country Head, CIB Country Head, Treasury	Country CRO Regional or Country Head (where present), TRM					

3. Decision Making Authority and Delegation

The Traded RTF is the formal mechanism through which the delegation of Traded Risk Authorities is made. The Global Head, TRM delegates authorities to designated individuals through this RTF.

Traded Risk Authorities are delegated as below:

Authority
1. GCRO
2. Global Head, TRM
3. TRM Management Team (Managing Directors)
4. TRM Leadership Team (generally Band 4 and Grade 5)
5. TRM Country Team (minimum Grade 5)

The Global Head, TRM is responsible for the Traded Risk authorities and TRM Head, Regulatory and Operational Effectiveness is responsible for embedding the key requirements into the detailed Traded Risk policies and related standards.

In addition, under the CIB Credit RTF, the Global Head, TRM receives Delegation of Credit Authority from the Co-Head, CRO CIB and CRO, ASEAN & South Asia.

Principles of Delegation of Authorities:

- Delegations do not remove the responsibilities of the delegator; and ongoing oversights are needed.
- Risk approval authority must not be delegated to individuals whose primary responsibilities relate to revenue generation.
- Authority recipients must have the required experience and judgement to exercise the proposed risk authorities and must either meet any applicable certification and/or experience requirements.
- Authority delegators are responsible for monitoring the quality of the risk decisions taken by their delegates and the ongoing suitability of their authorities.

The Global Head, TRM formalises the delegation of authorities to designated individuals via:

- **Delegation of Traded Authority (DTA)** letters. Only Senior Risk Managers (Band 4 or higher) may further delegate their authorities to team members. Delegation to Band 7 individuals must be approved by TRM Management team.
- **Delegation of Credit Authority (DCA)** letters. Details of the delegated authority matrices is included in the [Credit Authorities Addendum](#) to the CIB Credit Risk Chapter.

The RFO will ensure that there is monitoring in place to ensure the appropriate use of DTAs and DCAs.

In addition, local entities (Board, ERC) may delegate country-specific traded or credit authorities if a Group DTA/DCA is already in place for a given individual. While local authorities are not subject to Group oversight, they may not be larger than those contained in the Group DTA/DCA.

4. Regulatory Obligations and Escalation Mechanism

4.1 Group-level Regulatory Obligations

The Global Head, TRM (or delegate) is responsible for ensuring 2LoD oversight and challenge of legal and regulatory risks associated with their respective areas of responsibility, as covered by the following areas of laws and regulations:

Table 3: Areas of regulation related to Traded Risk

Area of Law and Regulation	Subject Matter Expert
Market Risk Rules	Global Head, TRM
Counterparty Credit Risk Rules	Global Head, TRM

The detailed set of laws and regulations is provided in Traded Risk Policy.

An annual attestation is conducted at Group level to facilitate periodic senior management oversight on Prudential Compliance attestation. Evidence of compliance along with resolution plan (if any) are noted for items with gaps as part of the attestation. The attestation completion is notified to Compliance and noted at CIB FRC for governance oversight.

5. Group Regulatory Interpretations

The governance of regulatory interpretations that have an impact on RWA/capital treatment of products is described below.

Table 4: Regulatory Interpretation Responsibilities

Market Risk (MR)			
Group-Solo MR capital-RWA regulatory requirements	First line – interpretation of requirements	Second line – review & validation of interpretation	Oversight & Governance
Internal Model Approach (IMA)	Market Risk Analytics team	Group Model Validation (GMV)	Traded Risk Models Assessment Committee (TMAC)
IMA add-ons	TRM Head, Market Risk	Global Head, TRM	CIB Financial Risk Committee (FRC)
Standardised Approach	TRM Head, Regulatory & Operational Effectiveness	Peer Reviewer vetted by Regulatory Interpretation Team	Regulatory Interpretation Forum and Regulatory Interpretation Committee

Counterparty Credit Risk (CCR)			
Group-Solo CCR capital-RWA regulatory requirements	First line – interpretation of requirements	Second line – review & validation of interpretation	Oversight & Governance
Internal Models Method	CCR Models team	GMV	TMAC
Other Model-related regulatory interpretations	CCR Models team	GMV	TMAC
Non-Model-related regulatory interpretations	TRM – CCR team	Peer Reviewer vetted by Regulatory Interpretation Team	Regulatory Interpretation Forum and Regulatory Interpretation Committee

Credit Valuation Adjustments (CVA)			
Group-Solo Market risk capital-RWA regulatory requirements	First line – interpretation of requirements	Second line – review & validation of interpretation	Oversight & Governance
CVA (SM/SA/BA)	Market Risk Analytics team	Peer Reviewer vetted by Regulatory Interpretation Team	Regulatory Interpretation Forum and Regulatory Interpretation Committee

6. Breach and escalation mechanism

The Global Head, TRM is responsible for developing an appropriate breach and escalation mechanism for those breaches or issues determined to be material. Escalation of breaches should be aligned with the response management requirements set out in the [Group Operational Risk Standard](#).

The Chapter Owner for prudential compliance attestation must escalate all material instances of non-compliance to the relevant Governance Committees and CIB FRC, to Compliance, and confirm that the Regulator was informed where needed.

Appendices Specific to this Framework

Appendix A: Traded Risk 2LoD Processes

Process	Description
Market Risk	
Framework and Market Risk Policies	The process provides framework, policy and standards oversight for the function. It ensures that TMR processes support the risk identification and management and remain compliant with various regulations.
Market Data Capture & Validation	Set up, capture and validation of instruments and curves in Asset Control feeding into the Group's system for risk management.
Risk Appetite Monitoring ¹	Risk appetite monitoring and control process focuses on setting and monitoring risk appetite in market risk management. Risk appetite thresholds are defined at a level apt to ensure that Group remains within risk appetite. These include measures that help manage correlation, concentrations and idiosyncratic risks.
Portfolio Controls	This process sets controls and governance requirements around TMR owned fields and associated roles, responsibilities in portfolio creation, review and maintenance in Portfolio Control Tool 2 (PCT2) with additional controls applied for non-standard portfolios, which is linked to Group Fraud Risk Management Policy.
Risk Reporting	In line with the requirements of Risk Reporting Standards (RRS), Market risk reporting process encompasses market risk information requirements, and designing, preparing and distributing market risk information to the intended recipients within expected timelines.
Stress Testing & Scenario Analysis	This process covers maintenance of Market Risk stress inventory, computation of stress results and management review and feedback on stress computations.
Market Risk Capital	This process covers the calculation and regulatory reporting of market risk regulatory capital.
Model Initiation Development and Monitoring	The Market Risk Model Life Cycle (MLC) refers to the actions taken to manage model risk for Market risk models. The MLC is an end-to-end process that a model goes through from inception to retirement that consists of 6 stages: initiation, development, independent validation, use and decommission. The MLC sets out the requirements and responsibilities for identification, measurement, mitigation and monitoring of Model risk.

¹ Includes limit setting for Algorithmic Trading, Algorithmic Trading processes.

Counterparty Credit Risk	
Portfolio Limits Setting and Review	To set portfolio limits to enforce diversification of CCR across multiple dimensions. Also ensure approval of portfolio limits in accordance with TRTF delegation of authorities and review at the agreed frequencies.
Transactional Approval	To approve trades and products in accordance with TRF and CIB Credit Risk Type Framework delegation of authorities and with the relevant standards and policies.
Stress Testing and Wrong Way Risk Management	To ensure that approved shocks are correctly implemented in CCR stress testing and wrong-way risk exposure calculation. Also, to review CCR stress testing and wrong-way risk exposures to ensure risks remain within appetite.
Monitoring and Excess Management	To investigate and remediate CCR limit breaches in a timely manner.
Reporting	This process covers the following: 1) Identifying the reporting requirements 2) Input collection of data for preparation and submission of report 3) Collation & processing of the submission of report 4) Validation, reconciliation & review of the submission of report 5) Submission of Report 6) Production
Model Initiation Development and Monitoring	The CCR MLC refers to the actions taken to manage model risk for CCR models. The MLC is an end-to-end process that a model goes through from inception to retirement that consists of 6 stages: initiation, development, independent validation, use and decommission. The MLC sets out the requirements and responsibilities for identification, measurement, mitigation and monitoring of Model risk.

Appendix B: Version Control

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Zeeshan Arif	Initial version created as part of the consolidation of standalone RTFs during the ERMF/RTF simplification exercise.	Material	SC PLC Board	1.0	7 Dec 2023
Renzo Baio	Section 3: Added the principles of Delegation of Authorities. ERMF Part C: <ul style="list-style-type: none"> Minor updates to the list of priority reports, the introduction of CIBRIR and retirement of the Underwriting Committee pack. Transfer of Origination and Distribution policy to CIB Credit 	Non-Material	Morgan Poquet	1.1	10 May 2024

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Sylvia Menezes	<p>Section 1.2: Re-introducing essential scope definition under Applicability.</p> <p>Section 2: To align oversight and management of Risk with the Group organisation design, “Hubs/ Regions” have been changed to “Clusters”.</p> <p>Section 3: Clarified Delegation of Traded Authority for Band 7 individuals.</p> <p>Added a sentence to ensure monitoring in place by RFOs for appropriate use of DCA and DTAs.</p> <p>Added a sentence to provide for instances where a country Board / ERC has an obligation to provide an independent DTA to a country risk manager.</p> <p>Section 4.1: With the transfer of Automated Trading Policy to Compliance, the reference to MIFID II RTS 6 under Table 3 has been removed.</p> <p>ERMF Part C:</p> <p>Transfer of Automated Trading policy to Compliance.</p>	Material	Sadia Ricke	2.0	13 Dec 2024

Note: Please refer to Part C of the ERMF for common appendices.

----- END OF CHAPTER FIVE -----

COMPLIANCE RISK TYPE FRAMEWORK

Chapter Number	Six – Part B of the ERMF
Principal Risk Type	Compliance Risk
Risk Framework Owner Name	Tracey McDermott
Risk Framework Owner Job Title	Group Head, Conduct, Financial Crime and Compliance (Group Head, CFCC)
Document Contact Name	Benjamin Hodges
Document Contact Job Title	Executive Director, Framework and Policy
Version Number	2.1

Delegation

For non-material changes to RTF	
Name	David Howes
Job Title	Global Head of FCC, Conduct & Compliance Framework

Contents

1. Overview of Compliance Risk Type Framework3

1.1 Compliance Risk management principles3

1.2 Overview of Compliance Risk3

2. Decision making authority and delegation3

3. Governance Committee oversight5

4. Regulatory Obligations and Escalation Mechanism5

4.1 Regulatory Obligations.....5

4.2 Breach and escalation mechanism6

5. Risk Identification, Assessment, Monitoring and Mitigation6

5.1 Dynamic Risk Identification6

5.2 Risk Assessment6

5.3 Risk Monitoring and Mitigation7

Appendices specific to this Framework.....8

Appendix A: Compliance Risk 2LoD processes and owners8

Appendix B: Compliance Risk references to other Principal Risk Type Frameworks.....8

Appendix C: Version Control8

Version Control Table

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Benjamin Hodges	Minor updates – reference to Regions replaced with Clusters, updated Section 2 with current Compliance Risk 2LOD Delegates job titles, updated Section 3 to align with Governance committee changes, and fixed broken link in Section 4.2	Non-material	David Howes	2.1	2 Dec 2024

The full version history is included in the RTF [Appendix C](#).

Chapter Six

1. Overview of Compliance Risk Type Framework

1.1 Compliance Risk management principles

All activities that the Group engages in must comply with the relevant country/local specific and **Extra-Territorial Regulations** (ETRs). The 1LoD must give due consideration to the apparent Compliance Risk and conduct risk at the point of making strategic choices and/or taking decision.

The Group's senior management is responsible for the effective management of Compliance Risk and the Group Head, **Conduct, Financial Crime and Compliance** (CFCC) has been designated as a Senior Manager under the UK Banking Reform Act Senior Managers' Regime and is the RFO for the Compliance Risk PRT.

Compliance Risk includes the risks associated with a failure to comply with all regulations that are applicable to the Group regardless of the issuing Regulatory Authority. Where Compliance Risk arises, or may arise, from failure to manage other PRTs, the oversight and management processes for that specific PRT must be followed. For example, where Compliance Risk arises from the risk of failure to manage ICS Risk, the approach set out in the ICS Risk Type Framework must be followed.

To help ensure consistency, wherever Compliance Risk is to be assessed and rated, the Regulatory Risk section of the GRAM in Part C of the ERMF must be used. This GRAM as outlined in the Operational & Technology Risk Type Framework is used both to rate the severity of crystallised events such as breaches of regulations and to assess exposure such as the potential impact of any such breaches due to ineffective controls.

Transaction-level decisions with respect to Compliance Risk are taken in line with the decision-making authorities set out under the Operational & Technology RTF or in the respective country/local addendum. These decisions are taken by the CFCC advisory teams aligned to the relevant businesses and functions.

1.2 Overview of Compliance Risk

Regulatory Authorities¹ issue regulations which the Group must comply with and expect reports and escalations of issues and breaches. The Group must have mechanisms for the identification and implementation of new and changing regulations, including assessment of their materiality, implementation of relevant processes and controls in the businesses and functions, monitoring of our compliance with the regulations and the ability to escalate and report breaches, if, and when they occur.

Compliance Risk advisory activities form the bridge connecting internal stakeholders, the Policy, and Standard Owners. Advisory is the vital activity of interpreting and explaining the Compliance Risk Appetite as it applies to a business, transaction, or function. It is often at this point that policy and standard owners will determine whether existing or planned activity fits within the Compliance Risk Appetite and will escalate, take steps to curtail activity or identify alternative lower- risk strategies to accomplish the business objective.

Compliance Risks are defined within the Non-Financial Risk Taxonomy that can be found [here](#).

Refer to [Appendix A](#) for details on 2LoD processes owned by CFCC.

2. Decision making authority and delegation

This RTF is the formal mechanism through which the delegation of authorities for Compliance Risk is made. The RFO delegates authorities to designated individuals or policy owners through this Chapter, including 2LoD ownership at a global business, product, and function level as well as cluster or country level. The 2LoD oversight and challenge responsibilities² for the Compliance Risk is as set out under Table 1 (2LoD delegate). These delegates have 2LoD oversight and challenge responsibilities of all Non-Financial Risk

¹ Regulatory Authorities mean local regulatory agencies or other government organization which can issue regulations and includes both Financial Services Regulators as well as other legislative bodies. To aid assignment of responsibility for monitoring changes to legislation, an individual rule book (such as the Banking Act) may be regarded as a Regulatory Authority. As such responsibility for monitoring changes can be assigned at an individual rule book level if necessary.

² 2LoD oversight and challenge responsibilities are set out in Table 1 of the ERMF.

Taxonomy Level 3 risks beneath the respective Level 2 Risk, except where specific risks³ relate to another PRT and therefore RFO.

Table 1: Compliance Risk 2LoD delegates ⁴

#	Non-Financial Risk Taxonomy Level 2 Risk	Second Line oversight and challenge responsibilities delegated to
1	Data Risk	Global Head, Data Conduct, CFCC
2	Conflicts of Interest	Global Head of Frameworks and Policies, CFCC
3	Non-Financial Regulatory Reporting	
4	Regulatory Conduct	
5	Market Conduct	Global Head, CFCC, Markets, Islamic Banking and ME
6	Client Conduct	Global Head, CFCC, Client Coverage and ASA

Each 2LoD delegate may further delegate this authority to Group CFCC Business and Functions advisory staff (CFCC Representative), except for exclusions as set out below for 2LoD oversight and challenge:

- **Data Quality (DQ)** risk: delegated to the Country Head of CFCC, while Group responsibilities are retained by the Global Head, Data Conduct, CFCC.
- **Chief Data Office (CDO)**: delegated to the Global Head, Data Conduct, CFCC.
- **Financial Crime Surveillance Operations (FCSO)**: delegated to the Global Head, AML.

Each CFCC Representative may further delegate their authority to CFCC officers of sufficient competency with responsibility for specific areas of business. Such delegation must be evidenced by respective RFO access rights in the M7 system, as set out [here](#).

For 2LoD processes owned by CFCC, the RFO delegates the responsibilities under each of the processes to the named roles under [Appendix A](#). The risk acceptance authority for risks rated Medium or above is delegated by the RFO as Process Universe Owner to the respective CFCC Process Owners as set out under [Appendix A](#).

Compliance Risk Acceptance and Treatment Plan authorities follow those as set out under the Operational & Technology RTF. The RFO delegates approval authority for the below Elevated Residual Risk Treatment Plans to the appropriate CFCC MT member:

- High with Treatment Plan less than or equal to 1 year.
- Medium with Treatment Plan greater than 1 year; and
- Medium with Treatment Plan less than or equal to 1 year ⁵.

³ Risk instances mapped to Level 3 risks: i) Regulatory Change; (ii) Identification and interpretation of Laws and Regulatory Requirements; or (iii) Governance of Regulatory Adherence, must be assigned to the appropriate RFO based on thematic risk to which the regulation relates.

⁴ Refer to the CFCC Frameworks [SharePoint](#) for detailed definitions and guidance for each Compliance Risk related Level 2 risk.

⁵ Approval authorities for Elevated Residual Risks that are Medium with TP less than or equal to 1 year can be further delegated to CFCC officers of sufficient competency with responsibility for specific areas of business.

3. Governance Committee oversight

A clear hierarchy of committee governs SCB's approach to managing Compliance Risk. An overview of Global, Hub, Cluster and Country Level Governance committees that provide primary oversight for Compliance Risk is shown below.

Table 2: Compliance Risk Governance Committee Oversight

Category	Level	Committee
Group	Board Level	BRC, AC
	Management Level	GRC, GNFRFC
	Business Level Committees	CIB NFRC, WRB RC
	Function Level Committees	CFCCR NFRC
Cluster	Management Level	HK & GNCA, SG & ASEAN, IN & South Asia, UK & Europe, US & Americas, ME & Pakistan, Africa
Country	Management Level	CRC / ERC

4. Regulatory Obligations and Escalation Mechanism

4.1 Regulatory Obligations

Approach to managing regulatory obligations

Areas of regulation can be broadly divided into two distinct categories; those issued by financial services Regulatory Authorities and those issued by non-financial services Regulatory Authorities. The Group is exposed to both categories of regulation. Roles and responsibilities differ as set out below, depending upon the category of regulation.

The relationship between the Regulatory Authorities, the types of regulations and RFO responsibilities can be represented as follows:

- Each RFO must identify the set of regulatory authorities for which they should be the 'Relevant Party,' and that RFO is responsible for the identification of regulations issued by that Regulatory Authority.
- An agreed list of regulatory authorities and relevant parties must be presented and agreed at the **Country Non-Financial Risk Committee (CNFRC)**. If there are any disputes as to which RFO should be the Relevant Party, this should be resolved by the CNFRC.
- For regulations issued by financial services Regulatory Authorities, CFCC is the Relevant Party and identifies new and amended regulations as and when issued in all countries where the Group has a presence and communicates the relevant regulatory obligations to the country RFO delegate.
- 2LoD RFO delegates are responsible for all aspects of policy definition and effectiveness review to help ensure risks are appropriately managed throughout the Group.
- Any disagreements relating to regulations being identified as material and not falling into any RTFs, must be escalated to the relevant CNFRC to determine 2LoD responsibilities.

The RFO (or delegate) is responsible for ensuring 2LoD oversight and challenge of risk of non-compliance with regulatory obligations associated with their respective areas of responsibility, as covered by the following areas of regulations⁶ issued by:

- Group regulators (i.e. PRA and FCA)
- Global policy/standard setters (e.g. Basel); and
- Country regulators (e.g. MAS, RBI)

⁶ These may include regulations issued in other forms by financial services regulatory authorities, including but not limited to guidelines and notices.

For regulations issued by financial services Regulatory Authorities and other regulators that may issue regulations pertaining to Compliance Risk (e.g. Competition and Anti-Trust or Privacy), the [Standard for Managing Regulatory Change](#)⁷ defines CFCC's approach to managing its regulatory obligations. This Standard sets out requirements for identifying, disseminating, and performing preliminary impact assessments of requirements issued by relevant regulators. Requirements in the Standard also include the effective interpretation of regulations and their codification into policies, as well oversight of implementation by the 1LoD. For regulations issued by financial services Regulatory Authorities, CFCC will also identify new and amended regulations as and when issued and communicate the relevant regulatory obligations to the applicable RFO delegate. The areas of regulations where CFCC does not act in a 2LoD capacity are specified in the respective RTF with appropriate ownership.

Communication with Regulators

Only staff who are authorised to do so can communicate with regulators (Authorised Staff) as set out in the [Group Communications with Regulators Standard](#).

Authorised Staff are expected to practice and demonstrate a high degree of compliance with the letter and spirit of rules to meet regulatory expectations. Engagement with regulators must be conducted in an open, honest, and cooperative manner with a view to ensuring that the Group understand their expectations and concerns and addresses them in a timely manner.

Locally, the advice of the relevant Country CFCC, **Central Point of Co-ordination** (CPC) or the Country-level RFO should be promptly sought if there is any doubt as to how a regulators request for information should be handled.

4.2 Breach and escalation mechanism

Any regulatory issues and breaches or potential regulatory breaches must be escalated to the RFO or the cluster or country delegate, who may assign a lead to manage, mitigate, and remediate the breach. The **Country Heads of CFCC** (CHoCFCC) will continue to maintain overall responsibility in ensuring the breach is effectively managed and remediated, including, where appropriate, reporting to the CNFRC.

Responsibilities and governance requirements for breaches as pertaining to Compliance Risk (except where the specific issue or breach relates to another PRT) will follow the [Regulatory Issues and Breach Recording Guidance](#) for the [OnePoint](#) system.

5. Risk Identification, Assessment, Monitoring and Mitigation

5.1 Dynamic Risk Identification

At the Group-level, a top-down periodic risk identification is required to assess the latest industry trends, regulatory requirements, and sector loss events. The output of this is communicated through the regulatory risk radar report by the RFO to the ERM Forum on a quarterly basis.

Within each country, in addition to the identification of material new and amended regulations, the country delegate of the RFO must determine a forward-looking view of prospective regulations and prospective changes in local regulatory focus for discussion with relevant management teams.

5.2 Risk Assessment

All businesses, functions and countries must assess Compliance Risk using the same descriptions of impact, and local country mitigation and remediation must be determined by country management as appropriate for materiality determined by the relevant process owner and RFO delegate. As a minimum, Compliance Risk is assessed on three scales:

- Monetary impact of fines and other penalties
- Impact to external stakeholders including regulators, markets, shareholders and clients
- Regulatory actions such as ongoing monitoring by and reporting to Regulatory Authorities

⁷ The CFCC approach to managing regulatory obligations has been enhanced for Group regulatory change, particularly in relation to large scale / complex regulation, with publication of a revised Managing Regulatory Change Standard effective 31 March 2022.

The CRTF will monitor the performance of first line against risk appetite, frameworks and policies and methods to assess the likelihood and/or materiality of impact. As part of the CRTF, **Compliance Risk Assessment** (CRA) must be carried out at a frequency commensurate with the materiality of the risk. The frequency and approach is to be agreed through the approval by the RFO of a documented methodology or methodologies. The determination of risk (as opposed to crystallised events) is a subjective assessment based on the skill, judgement and expertise of the relevant delegate of the RFO. It is the responsibility of the process owners, whether first or second line, to remediate any material areas of risk which are assessed to be outside risk appetite by the relevant second line. This remedial action must be completed to the satisfaction of the second line.

The RFO or delegate maintains an inventory of forward-looking assessments (portfolio reviews and stress tests) conducted, which includes information on the type of portfolio review or stress test conducted, when the review was conducted, coverage of the review, and recipients of these reviews. To be clear, the CRA does not replace the RCSA defined within the Group OR Standard but is a second-line assessment of Compliance Risk emanating from the first line. The Compliance **Enterprise-wide Risk Assessment** (EWRA) is a Group-wide risk assessment undertaken at a periodic interval (e.g., annually) to assess the compliance risk exposures and the associated control design and effectiveness measure through a defined methodology.

5.3 Risk Monitoring and Mitigation

Risk mitigation takes place through the process of identification of material new and amended regulations and the implementation of necessary process and control changes to address these. Processes, controls and control monitoring are governed by the O&T RTF, and any elevated risks will be governed through the relevant Non-Financial Risk Committees.

Appendices specific to this Framework

Appendix A: Compliance Risk 2LoD processes and owners

Details of the processes owned and executed by CFCC can be found [here](#).

A key activity that is not included as a process is the regulatory advisory activity carried out across the Group. This is because it is fundamentally reliant on the skill, judgement, and expertise (rather than following a process) of the relevant CFCC advisor to interpret the regulations and offer advice.

Appendix B: Compliance Risk references to other Principal Risk Type Frameworks

This RTF references all other PRTs which have 2LoD responsibilities of Compliance Risk. In addition to these, there are specific references to other Risk Type Frameworks as set out below:

Referenced PRT		Cross Reference Context
1	Operational and Technology RTF	Capital for Compliance Risk is Pillar 2A under Operational Risk
2	Operational and Technology RTF	Role of O&T Risk Type Framework in monitoring the control environment of the Risk Framework
3	Environmental, Social and Governance and Reputational RTF	Interface to Reputational Risk where a regulatory breach occurs

Appendix C: Version Control

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Zeeshan Arif	Initial version created as part of the consolidation of standalone RTFs during the ERMF/RTF simplification exercise.	Material	SC PLC Board	1.0	7 Dec 2023
Renzo Baio	<ul style="list-style-type: none"> Section 3: Minor wording changes to delegation and updates to the RFO access rights in M7 due to bridge decommissioning Removed reference to risk sub-types and aligned to L2 risks as per Risk Taxonomy. Appendix A: Replaced Compliance Risk 2LoD processes and owners with SharePoint hyperlink. Part C: <ul style="list-style-type: none"> C1 Appendix: Removal of Data Conduct as it is no longer a Risk Sub Type C3 Appendix: Update based on the approved Priority Report scope from BCBS239 review as of end-2023 	Material	Sadia Ricke	2.0	24 May 2024

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Benjamin Hodges	Minor updates – reference to Regions replaced with Clusters, updated Section 2 with current Compliance Risk 2LOD Delegates job titles, updated Section 3 to align with Governance committee changes, and fixed broken link in Section 4.2	Non-Material	David Howes	2.1	2 Dec 2024

Note: Please refer to part C of ERMF for common appendices.

----- END OF CHAPTER SIX -----

FINANCIAL CRIME RISK TYPE FRAMEWORK

Chapter Number	Seven – Part B of the ERMF
Principal Risk Type	Financial Crime
Risk Framework Owner Name	Tracey McDermott
Risk Framework Owner Job Title	Group Head, CFCC
Document Contact Name	Prince Bediako
Document Contact Job Title	Director, CFCC Governance
Version Number	1.2

Delegation

For non-material changes to RTF	
Name	David Howes
Job Title	Global Head of FCC, Conduct & Compliance Framework

Contents

1. Overview of Financial Crime Risk Type Framework3

2. Three Line of Defence Roles and Responsibility3

3. Governance Framework4

3.1 Decision Making Authority and Delegation.....4

3.2 Governance committee oversight at Group, Cluster and country level4

4. Regulatory Obligations and Escalation Mechanism5

4.1 Group-level Regulatory Obligations5

4.2 Country-level Regulatory Obligations.....5

4.3 Breach and escalation mechanism5

5. Risk Identification, Assessment, Monitoring and Mitigation5

5.1 Dynamic Risk Identification5

5.2 Risk Assessment5

5.3 Risk Monitoring and Mitigation5

Appendices specific to this Framework.....6

Appendix A: Financial Crime Risk 2nd LoD Oversight & Challenge RFO Delegations6

Appendix B: Financial Crime processes owned by the CFCC Function6

Appendix C: Business / Function owned processes mapped to Financial Crime6

Appendix D: Version Control.....7

Version Control Table

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Prince Bediako	Non-material with some edits based on organisational changes e.g. removal of regional layer and replaced by reference to Clusters.	Non-Material	David Howes	1.2	2 Dec 2024

The full version history is included in the RTF [Appendix D](#).

Chapter Seven

1. Overview of Financial Crime Risk Type Framework

Financial Crime (FC) risk management is built on a risk-based approach, meaning the risk management plans, processes, activities, and resource allocations are determined according with the level of risk. The **FC RTF** (this Chapter) outlines the governance and risk management approach unique to the PRT.

In respect of FC risk management, the Group will:

- establish operating standards and control processes reasonably designed to create compliance with applicable FC, legal and regulatory requirements and in line with Group **Risk Appetite** (RA); and
- support governments, law enforcement agencies and international bodies in combating FC.

2. Three Line of Defence Roles and Responsibility

This Chapter reinforces clear accountability and roles for managing risk through the 3LoD model outlined in the ERMF.

As the Second LoD, CFCC provides independent challenge, guidance, and oversight of the First LoD. CFCC set Policies and Standards which the First LoD must follow, including where teams within CFCC own First Line processes.

The CFCC Function in its capacity as Second LoD has process owner responsibilities as detailed in Appendix B. These processes are subject to the appropriate independent challenge and oversight as specified in the ERMF.

Figure 1: Financial Crime - Overview of the Three Lines of Defence & Committee Governance

	Standard Chartered PLC Board						
	Audit Committee (AC) / Board Risk Committee (BRC)						
	Group Financial Crime Risk Committee (GFCRC) / Group Risk Committee (GRC)						
	Country Financial Crime Risk Committees (CFCRC) / Country Non-Financial Risk Committees (CNFRC)						
	First LOD (owns and manages risk)			Second LOD (oversight and challenge)			Third LOD (independent assurance)
Client-businesses	Products	Functions	Client-businesses	Products	Functions		
Global	Client Business CEO or Global Business Head	Global Product Head	Global Functional Heads	RFO (Group Head, CFCC)			Group Internal Audit
Cluster	Cluster Business CEO or Cluster Business Head	Cluster Product Head	Cluster Functional Head	Cluster Head, FCC or Chief Compliance Officer			
Country	Country Business CEO or Country Business Head	Country Product Head	Country Functional Heads	Country RFO (Country Heads, FCC)			

3. Governance Framework

3.1 Decision Making Authority and Delegation

The FC RTF is the formal mechanism through which delegations of FC risk authorities are made.

The Group Head, CFCC is the Group Money Laundering Reporting Officer and holds the SMR 17 responsibilities for the Group.

The RFO delegates authorities to designated individuals or Policy Owners through this Chapter, including second line ownership at a global business, product, and function level as well as Cluster or country level.

Through this Chapter the RFO further delegates overall Second Line oversight and challenge responsibilities¹ for the Financial Crime risk as set out under [Appendix A](#) (second line delegate).

Each second line delegate may further delegate this authority to **Group CFCC Business and Function advisory staff** (CFCC Representative). At country level, the second line delegate may delegate this authority to the Country RFO who may further delegate this authority to country CFCC Representatives.

Each CFCC Representative (at Group or country) may further delegate² their authority to CFCC officers of sufficient seniority (they deem appropriate) with responsibility for specific areas of business.

For second line (Financial Crime) processes owned by CFCC, the RFO delegates the responsibilities under each of the processes to the named roles outlined in [Appendix B](#).

Financial Crime risk acceptance and treatment plan authorities follow those as set out under the Operational & Technology RTF³. The RFO delegates approval authority for the below Elevated Residual Risk Treatment Plans to the Global Head of FCC, Conduct & Compliance:

- high with Treatment Plan less than or equal to 1 year;
- medium with Treatment Plan greater than 1 year; and
- medium with Treatment Plan less than or equal to 1 year.

The RFO delegates authorities to the Head, CFCC Governance (or Director, CFCC Governance) to approve updates to linked internal and external FC documents, disclosures and statements, for example (but not limited to), ERM Forum CFCC “Heatmaps”, Risk Factors disclosures, annual Bank disclosures, etc.

The RFO (or the Global Head, CFCC, WRB GCNA or Global Head, CFCC, CIB, ASA and AME) appoints Country Heads, FCC (and where applicable FCC Cluster Heads) for the management of FC locally (or at Cluster level) and delegates authorities required to discharge their responsibilities. The Country Head, FCC (and where applicable FCC Cluster Heads), as the appointed Country RFO is responsible for ensuring compliance with this RTF at hub, branch or subsidiary level.

Delegators should maintain evidence of their onward delegation in the form and format they deem appropriate. Delegators should also ensure that any delegation is to an individual with sufficient seniority and skill to perform the delegated activity and/or role.

3.2 Governance committee oversight at Group, Cluster and country level

A clear hierarchy of committee responsibilities governs the Group’s approach to managing Financial Crime. Oversight of FC within the Group is governed through:

- Board Level oversight at the **Audit Committee** (AC) and the **Board Risk Committee** (BRC).
- Senior Management oversight at the **Group Financial Crime Risk Committee** (GFCRC) for AML, Sanctions and ABC and the **Group Non-Financial Risk Committee** (GNFRC) for Fraud; and
- Country-CEO level engagement at **Country Financial Crime Risk Committees** (CFCRC), **Country Non-Financial Risk Committees** (CNFRC). Oversight of FC risk may also be provided by country Executive Risk Committees (ERC) or Country Risk Committees (CRC).

¹ Second line oversight and challenge responsibilities are set out in the ERMF

² Delegate in line with ERMF (Source of Authorities)

³ Risk Acceptance and Treatment Plan Escalation, Approval and Closure Authorities responsibilities are set out by Operational Risk Financial Crime – Chapter 7

4. Regulatory Obligations and Escalation Mechanism

4.1 Group-level Regulatory Obligations

The RFO (or delegate) is responsible for second line oversight and challenge ensuring compliance with Financial Crime regulatory obligations.

For regulations, issued by Financial Services Regulators, Compliance will identify new and amended regulations as and when issued and communicate the relevant regulatory obligations to the applicable RFO delegate.

Policy Owners, as **Subject Matter Experts** (SMEs), are responsible for identifying regulatory obligations relevant for their area of responsibility and the scope of the Policy, in line with Policy Owner responsibilities in section 8.5 of the ERMF.

4.2 Country-level Regulatory Obligations

Requirements for country-level regulatory obligations, and roles and responsibilities are specified in section 16.3 and 16.4 of the ERMF.

4.3 Breach and escalation mechanism

The RFO or delegate is responsible for developing a breach and escalation mechanism for issues determined to be material by the Country RFO.

Any regulatory issues and breaches or potential regulatory breaches must be escalated to the RFO or the cluster or country delegate who may assign a lead to manage, mitigate, and remediate the breach. In country, the Country Head, CFCC (where relevant, Country Chief Compliance Officer) will continue to maintain overall responsibility in ensuring the breach is effectively managed and remediated, including, where appropriate, reporting to the relevant country committee responsible for FC oversight.

5. Risk Identification, Assessment, Monitoring and Mitigation

5.1 Dynamic Risk Identification

On an ongoing basis Policy Owners are responsible for ensuring ongoing compliance with applicable financial crime legal and regulatory obligations.

The output of the above processes is communicated by the RFO (or Global Head, FCC, Conduct & Compliance Framework) to the ERM Forum.

5.2 Risk Assessment

The Group monitors enterprise-wide FC risks through the FCC Risk Assessment. The Financial Crime risk assessment is a Group-wide FC risk assessment undertaken annually to assess the inherent financial crime risk exposures and the associated processes and controls by which these exposures are mitigated.

5.3 Risk Monitoring and Mitigation

Risk monitoring follows the same structure as risk appetite monitoring.

Risk mitigation takes place through the process of identification of new and amended regulations and the implementation of necessary process and control changes to address these. Processes, their controls and control monitoring are governed by the Operational & Technology Risk Type Framework, however the FC risk created by processes will be reported and governed under this framework.

Appendices specific to this Framework

Appendix A: Financial Crime Risk 2nd LoD Oversight & Challenge RFO Delegations

The table below lists the 2nd Line of Defence Oversight and Challenge responsibilities (as detailed in the Operational Risk Standard) for the Financial Crime Level 2 Risks in the [Non-Financial Risk Taxonomy](#).

Non-Financial Risk Taxonomy Level 2 Risk	FCC Owned Processes		Function Owned Processes		Business Owned Process	
	Group	Country	Group	Country	Group	Country
Anti Money Laundering (and Terrorist Financing)	Global Head, AML	Country Head, FCC	Global Head, AML	Country Head, FCC	Corporate & Investment Banking (CIB) <ul style="list-style-type: none"> Head CFCC CCIB, AME, Group Islamic, FM and TM Global Head, CFCC Advisory, TB, DCDA Chief Compliance Officer, SC Ventures Global Head of CIB Advisory Client Coverage 	Country Head, FCC
Sanctions			Global Head, FCC, Sanctions, High Risk Clients & Emerging Threats			
Anti Bribery and Corruption			Head, FCC, Intelligence & Investigations Unit			
Internal Fraud External Fraud					Wealth and Retail Banking (WRB) <ul style="list-style-type: none"> Chief Compliance Officer, Affluent and Wealth Management Head CFCC Advisory, PBB Client Coverage Head CFCC Advisory, PBB Products and Banking Operations Head CFCC Advisory, PBB Digital Data 	

Appendix B: Financial Crime processes owned by the CFCC Function

A list of processes owned⁴ and executed by the CFCC Function in support of Financial Crime risks along with a corresponding description can be found [here](#).

Appendix C: Business / Function owned processes mapped to Financial Crime

A list of Business / Function owned processes with identified risks mapped to Financial Crime risks can be found [here](#).

⁴ Ownership of following processes moved to the 1LoD in 2021 as part of the transfer of operational surveillance activities: SSI Name Screening, Transaction Monitoring, Transaction Screening, AA Name Screening, AA Transaction Monitoring, AA Transaction Screening and MI and Data Management (MDIDM). FCC retains ownership for FCC Act and Sanctions Act.

Appendix D: Version Control

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Zeeshan Arif	Initial version created as part of the consolidation of standalone RTFs during the ERMF/RTF simplification exercise.	Material	SC PLC Board	1.0	7 Dec 2023
Renzo Baio	<ul style="list-style-type: none">Non-material with some edits on delegations and updates to 2nd Line oversight and challenge delegations in Appendix ARemoved reference to risk sub-types and aligned to L2 risks as per Risk Taxonomy.	Non-Material	David Howes	1.1	26 Apr 2024
Prince Bediako	Non-material with some edits based on organisational changes e.g. removal of regional layer and replaced by reference to Clusters.	Non-Material	David Howes	1.2	2 Dec 2024

Note: Please refer to Part C of the ERMF for common appendices.

----- END OF CHAPTER SEVEN -----

OPERATIONAL & TECHNOLOGY RISK TYPE FRAMEWORK

Chapter Number	Eight – Part B of the ERMF
Principal Risk Type	Operational and Technology Risk
Risk Framework Owner Name	Adrian Munday
Risk Framework Owner Job Title	Global Head, Operational, Technology & Cyber Risk
Document Contact Name	Margaret Norden
Document Contact Job Title	Global Head, OTCR, Framework & Stress Testing
Version Number	2.1

Contents

1. Overview of the Operational & Technology Risk Type Framework3

1.1 Operational & Technology Risk Management Principles3

1.2 Overview of Operational & Technology Framework3

1.3 Updates to Framework.....4

2. Three Lines of Defence Roles and Responsibility4

3. Governance Framework4

3.1 Decision Making Authority and Delegation.....4

3.2 Governance Committee Oversight at Group, Cluster and Country level.....5

4. Regulatory Obligations and Escalation Mechanism5

4.1 Group-level Regulatory Obligations5

4.2 Breach and escalation mechanism5

5. Scenario Analysis and Capital Adequacy6

5.1 Scenario Analysis6

5.2 Capital Adequacy.....6

Appendices Specific to this Framework7

Appendix A: Operational & Technology Risk SME Delegations7

Appendix B: Version Control8

Version Control Table

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Eonike Lema	<ul style="list-style-type: none">Updated name of RFO Owner nameTable1: Updated table to reflect changes in Group Risk Committee (GRC) One-Down Committees.Appendix A: Removed "Interim" from Global Head OTCR, Resilience Risk.	Non-material	Adrian Munday	2.1	5 Dec 2024

The full version history is included in the RTF in [Appendix B](#).

Chapter Eight

1. Overview of the Operational & Technology Risk Type Framework

1.1 Operational & Technology Risk Management Principles

The **O&T RTF** (this Chapter) outlines the governance and risk management approach unique to Operational & Technology Risk. Operational & Technology Risk is defined as the potential for loss resulting from inadequate or failed internal processes, technology events, human error or from the impact of external events (including legal risks). This Chapter is built on a risk-based approach, meaning the risk management plans, processes, activities, and resource allocations are determined in accordance with the level of risk.

The first line, when formulating business strategy and planning, must consider and address Operational & Technology Risk at the point of strategic choices and/or decision making. This should also include consideration of the impact of decisions on the design and operational effectiveness of the related system of controls.

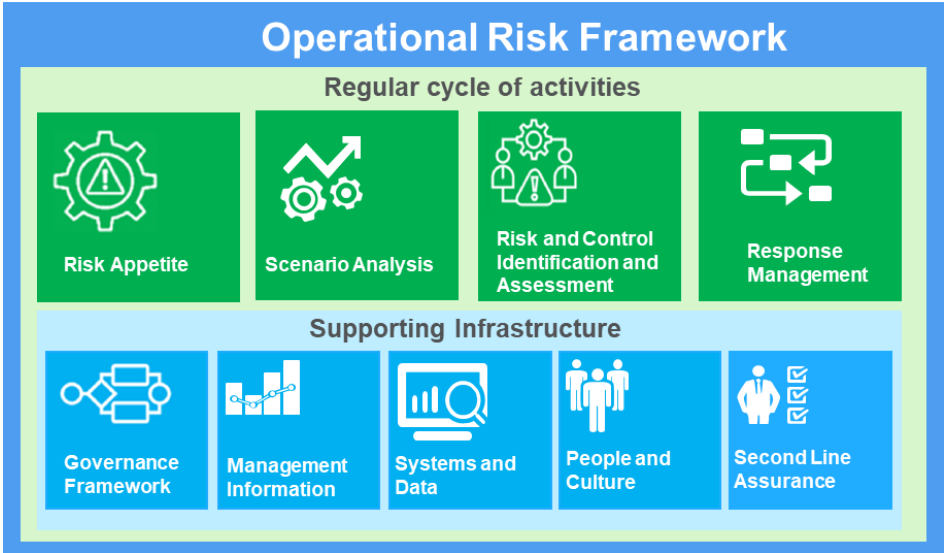
- Risk appetite and scenarios should be used strategically to help planning and business management.
- There should be a top-down, complete, and consistent approach to risks and controls through the **Risk and Control Self-Assessment (RCSA)** process.
- The RCSA process involves objective assessments of risks based on client impact and likelihood, more focus on material risks, more thinking on control design rather than simply testing, and tools to allow countries to prioritise local actions.
- When an operational risk event occurs, there needs to be rapid escalation and root-cause reviews, tracked to completion.
- People are skilled and rewarded for good risk management behaviour.
- The data and system encourage good risk management behaviour.
- Given the pervasive and strategic importance of technology in the Group’s business model, ensure appropriate prominence and amplification in the governance structures to support the identification, measurement, monitoring and control for technology related risks.
- Second line independent review is risk-based and proportionate.

Climate Risk may be material to Operational Risk exposures due to impacts from physical and transition risks on the Groups operations including branches, offices and data centres, the Group’s ability to service clients and impact on vendor operations. The **RFO** (or SME) is responsible for monitoring Climate Risk profile associated with Operational Risk and providing actions plans as applicable.

1.2 Overview of Operational & Technology Framework

The O&T Framework applies to all PRTs across the Group. It must be implemented in all business segments / functions, banking subsidiaries and branches.

Figure 1: Cycle of activities



1.3 Updates to Framework

The Global Head, Operational, Technology & Cyber Risk (OTCR) can authorise non-material changes to the O&T Framework.

2. Three Lines of Defence Roles and Responsibility

The O&T Chapter reinforces clear accountability and roles for managing risk through the Three LoD model.

The 1LoD is the business segments and functions accountable for the management of the activities of the Group. At the country, regional and global level, the CEO, Business, Product and Functional Heads form the 1LoD for Operational and Technology Risks.

The 1LoD is required to comply with the applicable laws and regulatory expectations, manage the risk that arises from first line activities and comply with policies set by the 2LoD. Senior management in the 1LoD is accountable for embedding a sound risk culture in their areas of responsibilities.

The 2LoD within OTCR¹, comprises of OTCR Business / Function Coverage Leads and OTCR SMEs who support the Global Head, OTCR.

- i. **Business / Function Coverage Leads** are accountable and responsible for effective 2LoD Risk management for their respective functions. These Coverage teams are responsible for the following activities:
 - Review, challenge and (where relevant) approval on business/function risk matters.
 - Approvals on risk decisions within business and function.
 - End to end oversight of risk performance.
 - Act as Single Point of Contact within 2LoD for first line across Businesses and Functions.
 - Approval of Risk Treatment Plans in line with the Appendix D – Risk Treatment Plan Escalation, Approval and Closure Authorities defined in the Group Operational Risk Standard.
- ii. **OTCR SMEs teams** are responsible for the following activities:
 - OTCR SMEs team will help, guide and support informed decision making and risk management with their specialist knowledge and expertise.
 - Set policies that the 1LoD must adhere to.
 - Confirm the effectiveness of their policies to the Global Head, OTCR.

For a number of risks under the Non-Financial Risk Taxonomy, the Global Head, OTCR as the RFO for O&T risks, places reliance on the designated **Senior Managers** who are outside the Risk function for 2LoD oversight responsibilities, including setting appropriate policies and supporting control standards, and approvals on risk decisions.

In those instances, the Global Head, OTCR retains 2LoD oversight accountability whenever the Senior Manager is responsible for both setting policy and executing processes in compliance with their own policy.

3. Governance Framework

3.1 Decision Making Authority and Delegation

The O&T RTF is the formal mechanism through which the delegation of Operational and Technology Risk authorities is made.

For a number of risks under the Non-Financial Risk Taxonomy, the Global Head, OTCR as the RFO for O&T risks, places reliance on the designated **Senior Managers** who are outside the Risk function for second line oversight responsibilities, including setting appropriate policies and supporting control standards, approvals on risk decisions. The designated Senior Manager may further delegate to the Policy Owners, including 2LoD ownership at a global business, product, and function level as well as regional or country level.

¹ For L2 risks - Transaction Processing Failure, Product Mismanagement, Change Mismanagement and Third-Party Mismanagement, Client Service Disruption, Technology.

The Global Head, OTCR also delegates authority to the Group and Country Head of OTCR to discharge the 2LoD authorities as defined in the job descriptions for oversight and challenge activities to assess the effectiveness of the risks and quality of its implementation.

Sub-delegation is to be updated in the Group OR management system for undertaking risk decisions. The Senior Manager must ensure that key risk decisions are only taken by individuals with the requisite skills, judgement, and perspective to ensure that the Group's risk / return objectives are met.

Formal reviews in the form of Policy Effectiveness Review of the delegations must be conducted by the delegator every year. Evidence of this review must be maintained by the delegator.

3.2 Governance Committee Oversight at Group, Cluster and Country level

A clear hierarchy of committee responsibilities governs the Group's approach to managing the O&T RTF. On behalf of the **Group Risk Committee (GRC)**, the **Group Non-Financial Risk Committee (GNFRC)** is responsible for governing **Non-Financial Risk (NFR)** across all functions, client segments and products excluding the NFR types of Financial Crime, Country Risk and Reputational Risk (Primary). Material NFRs must be escalated from the GNFRC up to the GRC as required.

Oversight of the O&T Framework is through the following Group and geographic committees:

Table 1: Governance Committee Oversight

Category	Level	Committee
Group	Board Level	BRC
	Management Level	GRC, SC Bank ERC, GRRRC, GFCRC, GNFRC, GALCO
	Business Level Committees	CIB NFRC, WRB RC, SCV RC
Cluster	Management Level	HK & GNCA RC, SG & ASEAN RC, IN & South Asia RC, UK & Europe RC, US & Americas RC, ME & Pakistan RC, Africa RC
Country	Management Level	CRC/ERC, CNFRC

4. Regulatory Obligations and Escalation Mechanism

4.1 Group-level Regulatory Obligations

The Global Head, OTCR (or delegate / SME) is responsible for ensuring 2LoD oversight and challenge of legal and regulatory risks associated with Prudential - Operational Risk and Operational Risk Rules.

For regulations, issued by Financial Services Regulators, Compliance will identify new and amended regulations as and when issued and communicate the relevant regulatory obligations to the applicable RFO delegate / SME.

4.2 Breach and escalation mechanism

Breaches of any applicable regulations for any of the Operational & Technology Level 2 / Level 3 risks must be escalated in line with the requirements set out in the [Operational Risk Policy](#) and [Standard](#). Where a breach occurs in a country, escalation should be to the delegate of the relevant Operational & Technology Risk SME.

Breaches should be discussed at the relevant governance committee with responsibility for the segment, product, function, or country (as per Table 1). Material breaches should be further escalated to the relevant Group-level governance committee. The relevant Operational & Technology Risk SME (or delegate) is responsible for this escalation.

Where there is a need for prompt reporting of the breach to a regulator, the breach should be escalated to the relevant Operational & Technology Risk SME, the Global Head, OTCR, and the GCRO prior to external disclosure. Similarly, in countries, the escalation should be to the Operational & Technology Risk SME delegate, the Country Head of OTCR, and to the Country Chief Risk Officer prior to external disclosure.

Material country breaches must be escalated to relevant Group individuals by the Operational & Technology Risk SME / delegate.

5. Scenario Analysis and Capital Adequacy

5.1 Scenario Analysis

At the start of the year, GNFRRC approves a Scenario Analysis Plan comprising of scenarios to quantify stress outcomes and / or to identify additional risk mitigations actions for the Group. The quantification of the scenarios further supports the assessment of the Group's capital adequacy as outlined below.

For Enterprise Stress Tests, stress testing should be carried out according to the requirements set out in the [Enterprise Stress Test Policy](#), as well as relevant standards and policies. In particular, stress testing is used to analyse the impact of climate change as well as to calibrate certain Group O&T RA metrics.

5.2 Capital Adequacy

Operational risk is subject to minimum requirements in accordance with the UK CRR² in order for the Group to operate within Risk Capacity. The Group implements the Standardised Approach to assess these requirements. On an annual basis, the Pillar 1 minimum requirement is calculated by the Group Finance Team and is included in the Group's ICAAP.

In accordance with the overall capital adequacy rule, an ICAAP is undertaken annually. Risks that are not covered, or not sufficiently covered, by Pillar 1, are assessed as part of the Pillar 2A assessment. This, together with the Pillar 1 CRR minimum requirements, forms the basis for determining the Group's **Total Capital Requirement** (TCR). The Global Head, OTCR can determine if any additional Pillar 2A add-on is required based on any material residual risks.

At a Group level, the Pillar 2 assessment for Operational Risk is produced by Group Operational Risk Stress Testing team. Countries are to be guided by their local Regulators where the approach varies from above.

Operational Risk's capital assessment includes consideration for operational risk arising in selected non-financial PRTs and Operational & Technology L2/L3 risks as per the Non-Financial Risk Taxonomy. The qualitative assessments consider the definition of the risk, risk appetite, relevant internal and external data as well as SME judgement. The Global Head, OTCR can determine if any additional Pillar 2A add-on is required based on material residual risk not adequately capitalised under the ICAAP.

The [Operational Risk Policy](#) and [Operational Risk Standard](#) further sets out the Group Level Scenario Analysis processes.

² UK Capital Requirement Regulation (CRR)

Appendices Specific to this Framework

Appendix A: Operational & Technology Risk SME Delegations

All SMEs are responsible for setting appropriate policies and supporting control standards.

Global Head, OTCR as the RFO for Operational & Technology Risk, place reliance on the designated Senior Managers who are outside the Risk function for setting appropriate policies and supporting control standards, and approvals on risk decisions.

Non-Financial Risk Taxonomy (Level2/3)	Definition	Subject Matter Experts
Transaction Processing Failure*	Potential for loss or adverse impact due to failures in the design or execution of client facing transaction.	Global Head, OTCR, Framework & Stress Testing
Product Mismanagement*	Potential for loss or adverse impact due to failure to design, approve and maintain appropriate products/services.	Global Head, OTCR, Framework & Stress Testing
Client Service Disruption*	Potential for loss or adverse impact due to the failure maintain or manage processes supporting client service.	Global Head, OTCR, Resilience Risk
Technology Risk*	Potential for loss or adverse impact due to technology failure (hardware, infrastructure, application)	Global Head, OTCR, TTO
Change Mismanagement*	Potential for loss or adverse impact due to failures in the planning, management, and implementation of change within the Bank.	Global Head, OTCR, Framework & Stress Testing
People Risk	Potential for loss or adverse impact due to failures relating to people management, including failure to have a diverse and inclusive workforce with the right capabilities and capacity and/or having inadequate employment practices and poor employee behaviour.	Chief Strategy and Talent Officer
Physical Safety and Security	Potential for loss or adverse impact due to the failure to create a safe, secure, and physically healthy environment for employees, associated persons, third parties and visitors.	Group Head, Property
Third Party Risk Mismanagement*	Potential for loss or adverse impact due to the failure to manage the onboarding, lifecycle and exit strategy of a third party.	Global Head, OTCR, Framework, & Stress Testing
Corporate Governance Standards	Risk of failing to comply with relevant corporate governance standards.	Group Company Secretariat

Board Governance	Risk of ineffective governance arrangements, oversight, decisions and/or approvals by the Board or Board Committees.	Group Company Secretariat
Listing Requirements	Risk of failing to comply with stock exchange listing requirements.	Group Company Secretariat
Shareholder Relations	Risk of ineffective management of shareholders relations (including shareholder communications, meetings, annual reports).	Group Company Secretariat
Financial Books and Records	Potential for loss or adverse impact due to failures to comply with requirements related to financial statements and disclosures.	Group Head, Finance
Financial Regulatory Reporting	Potential for loss or adverse impact due to failure to comply with financial regulatory reporting requirements by submitting inaccurate, incomplete, and/or untimely reports to the relevant regulatory authority (excluding tax reporting obligations).	Group Head, Finance
Tax Risk	Potential for loss or adverse impact due to failure to comply with tax filing obligations.	Group Head, Tax
Legal Enforceability	Risk of the Bank being unable to enforce its contractual rights.	Group General Counsel

* For these L2 risks, **OTCR Business / Function Coverage Leads** are accountable and responsible for effective 2LoD Risk management for their respective functions (Refer Section 2i above).

Appendix B: Version Control

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Zeeshan Arif	Initial version created as part of the consolidation of standalone RTFs during the ERMF/RTF simplification exercise.	Material	SC PLC Board	1.0	7 Dec 2023
Renzo Baio	<ul style="list-style-type: none"> Section 1: Reintroduced definition for O&T Risk within the chapter for added clarity. Section 3.1: Repositioned reliance on SMEs from section 1.3 Removed reference to sub risk-types and aligned to L2 / L3s as per the Non-Financial Risk Taxonomy. Appendix A: Updated to reflect Risk and ownership as L2/L3s and removed reference to RSTs. <p>Part C: Appendix C1 and C2: Inclusion of Third Party risk RST and policy under O&T risk.</p>	Material	Sadia Ricke	2.0	30 May 2024
Eonike	<ul style="list-style-type: none"> Updated name of RFO Owner name Table1: Updated table to reflect changes in Group Risk Committee (GRC) One-Down Committees. Appendix A: Removed "Interim" from Global Head OTCR, Resilience Risk. 	Non-material	Adrian Munday	2.1	5 Dec 2024

Note: Please refer to part C of ERMF for common Appendices.

----- END OF CHAPTER EIGHT -----

MODEL RISK TYPE FRAMEWORK

Chapter Number	Nine - Part B of the ERMF
Principal Risk Type	Model Risk
Risk Framework Owner Name	Jason Forrester
Risk Framework Owner Job Title	Global Head ERM & Deputy CRO SC Bank
Document Contact Name	Mark Green
Document Contact Job Title	Global Head of Model Risk Management
Version number	1.2

Contents

1. Overview of the Model Risk Type Framework..... 3

1.1 Model Risk Management Principles..... 3

1.2 Overview of Model Risk..... 3

2. Model Risk Scope 4

2.1 Model Families 4

2.2 Geographies..... 6

3. Three LoD – Responsibility and Governance Committee Oversight 6

4. Decision making Authorities and Delegation..... 7

5. Regulatory Obligations..... 7

5.1 Group-level Regulatory Obligations 7

5.2 Breach and escalation mechanism 8

Appendices specific to this Framework 9

Appendix A: Version Control 9

Version Control Table

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Mark Green	Consolidation or Unification of MFS for Vendor, IRRBB, Liquidity and Capital MFS into a new MFS Liquidity IRRBB Capital Management and Reporting GMFS Updates of MFS linkages Adding clarity to Quantitative Methods meaning categorising Models and DQMs per PRA SS 1/23 MRM Principles drop-down, Cluster level updates to Framework visualization	Non-Material	Jason Forrester	1.2	11 Dec 2024

The full version history is included in the RTF [Appendix A](#).

Chapter Nine

1. Overview of the Model Risk Type Framework

1.1 Model Risk Management Principles

The Model RTF (this Chapter) outlines the governance and risk management approach unique to Model Risk. The Model Risk Framework is built on a risk-based approach, meaning the risk management plans, processes, activities, and resource allocations are determined in accordance with the level of risk and is consistent with the three LoD model prescribed by the ERMF.

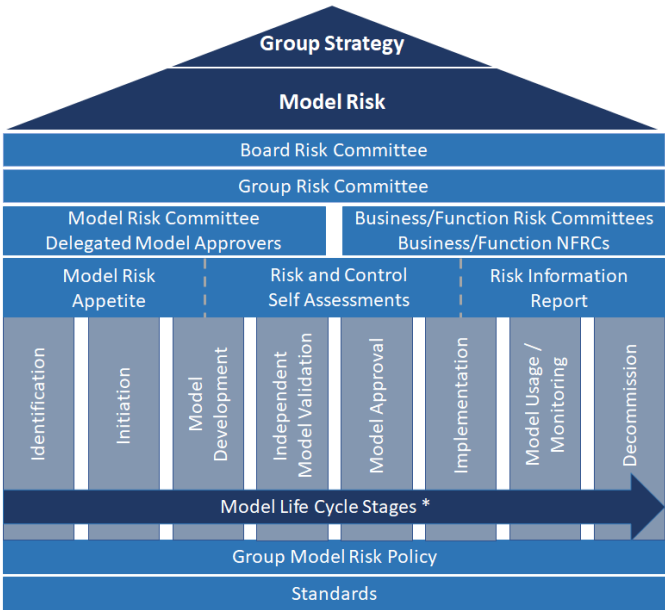
The first line, which is the business Model Sponsors, Model Owners, Model Users, and applicable Process Owners, must give due consideration to the apparent Model Risk at the point of strategic choices, decision making and conduct risk management.

Below are the main principles that will form the basis of the Model Risk Management:

- All models, within scope, used in processes within the Group should be:
 - Duly and promptly identified and registered in the model inventory by 1LoD
 - Adhering to the requirements of the policy and standards for the various stages in the **Model Life Cycle** (MLC) as applicable
 - Independently validated and regularly monitored as per approved policy and standards to ensure models continue to be fit for their intended usage
- Within the parameters and principles defined within this chapter and its supporting policy, the 1LoD should have adequate flexibility in the governance of their respective models to ensure effective risk management.
- Model risk management should be conducted by competent, skilful individuals with adequate model, business, and product knowledge.
- The organisational design supporting model risk management should ensure appropriate management of potential conflicts of interests.

1.2 Overview of Model Risk

Figure 1: Overview of Model Risk



*The flow of the generic MLC stages described in the above framework could be adjusted as per the specific nature and requirements of each Model Family.

The Group's model risk framework works through a systematic network of processes and governances as noted in the diagram above. The overarching guidance is described within this Chapter.

Model Risk Committee (MRC) is appointed by the **Group Risk Committee** (GRC) to ensure effective measurement and management of model risk in line with internal policies and model risk appetite. Model risk is closely monitored by tracking the Board approved model risk appetite metrics, supported by RCSA in the O & T Risk Framework and model risk related risk information reporting.

Whilst the MRC typically delegates model approval to **Delegated Model Approvers** (DMA), it reserves the right to approve models with perceived heightened model risk. The appointment of DMA, by the MRC, is based on specific areas of expertise they possess within the model landscape. For example, certain credit risk models are approved by the **Credit Model Assessment Committee** (CMAC), certain traded risk models are approved by the **Traded risk Model Assessment Committee** (TMAC) and certain financial crime compliance models are approved by the **Financial Crime Compliance Model Assessment Committee** (FCCMAC).

The Group has rolled out the [Group Model Risk Policy](#) (GMRP) to manage model risk arising across the generic MLC. GMRP should be read in conjunction with applicable [Group Model Risk Standards](#) (GMRS), [Group Deterministic Quantitative Methods Standards](#) (GDQMS) and **Model Family Standards** (MFS). The Standards explain how the policy requirements are to be met and where applicable, describe any adjustments to the MLC specific to the requirements of each Model Family.

GMRP specifies the definition of models and scope of the model landscape. Models within the definition are identified and developed as per GMRP, and applicable standards. Independent validation of the models provides opinion and grading of the models, and they are recommended for approval by the DMAs. Models are monitored to ensure it is used for the approved usages.

Model Risks are defined within the Non-Financial Risk Taxonomy that can be found [here](#).

2. Model Risk Scope

Models are a subset of all quantitative methods and variety of those such as systems, approaches, calculators designed standalone or in applications and used in operations. Model outputs are estimates, forecasts, predictions, or projections, which themselves could be the input data or parameters of others. Technology and data processing environment become more complex and statistically orientated, thus enable **Deterministic Quantitative Methods** (DQM) such as decision-based rules or algorithms to support important business decisions and give rise to Model Risk.

The scope of applicability of the Model Risk is defined by the dimensions of a group of Model Families (each representing a particular Model and/or DQM type) and the geographies the framework has been rolled out to. A variety of model types are used across the Group i.e., model outputs are used to support decisions made in relation to business activities, strategic decisions, pricing, financial, risk, compliance and financial crime, capital, and liquidity management, further defined in Model Families.

2.1 Model Families

Scope of Model Risk is defined, in part, by the approved Model Families, which formally categorise a variety of in scope model types used by the Group, including the consequent differences in model risk manifestation and associated risk management approach. Each family is supported by a **Model Family Standard** (MFS), which further details the respective model risk management processes. MFS are co-owned by the 1LoD (Model Owner) and 2LoD (Model Risk Management), with sections pertaining to requirements solely owned by the Model Risk Management function.

Model Families in scope for model risk will be reviewed annually as part of the Model Risk RTF review cycle and/or the GMRP refresh cycle. Out-of-cycle reviews may be performed as required should there be a significant change in the model landscape, such as when new model types or new model use cases emerge. The list of Model Families is outlined in Table 1 below:

Table 1: List of Model families

Model Family	Definition	Group Model Family Standards
Credit Risk Internal Ratings Based (IRB) & Scorecards	Potential for loss and/or misstatement arising from the misestimation of credit risk due to errors in the development, implementation or usage of credit risk IRB models and scorecards.	<u>Credit Risk IRB Models and Credit Risk Scorecards Standard</u>
Credit Risk IFRS9	Potential for loss and/or misstatement arising from the misestimation of credit risk due to errors in the development, implementation, or usage of credit risk IFRS9 models.	<u>Credit Risk IFRS9 ECL Models Standard</u>
Market Risk	Potential for loss and/or misstatement arising from the misestimation of market risk due to errors in the development, implementation, or usage of these models.	<u>Market Risk Standard</u>
Counterparty Credit Risk	Potential for loss and/or misstatement arising from the misestimation of counterparty credit risk due to errors in the development, implementation, or usage of these models.	<u>Counterparty Credit Risk Standard</u> <u>SIMM Model Framework Standard</u>
FM Pricing Models	Potential for loss and/or misstatement arising from the misestimation of FM pricing due to errors in the development, implementation, or usage of these models.	<u>FM Pricing Models Standard</u> <u>CIB Markets Deterministic Quantitative Methods (DQM) Standard</u>
Financial Crime Compliance (FCC)	Potential for regulatory penalties and financial loss and/or misstatement arising from the misestimation of financial crime compliance due to errors in the development, implementation, or usage of these models.	<u>FCC Standard</u>
Operational Risk	Potential for regulatory penalties and financial loss and/or misstatement arising from the misestimation of operational risk due to errors in the development, implementation, or usage of these models.	<u>Operational Risk Standard</u>
Liquidity, Interest Rate Risk in the Banking Book (IRRBB), Capital Management and Reporting	Potential for regulatory penalties and financial loss and/or misstatement arising from the misestimation of liquidity risk, IRRBB and capital risk due to errors in the development, implementation, or usage of these models.	<u>Liquidity, IRRBB, Capital Management and Reporting Standard</u>
Enterprise-Wide Stress Test (EWST) Financial Projections	Potential for regulatory penalties arising from the misestimation of financial projections used in the stress testing due to errors in the development, implementation, or usage of these models.	<u>EWST Financial Projection Standard</u>

Economic Scenarios	Potential for regulatory penalties arising from the misestimation of economic scenarios due to errors in the development, implementation, or usage of these models.	<u>Economic Models Standard</u>
Pension Risk	Potential for regulatory penalties and financial loss and/or misstatement arising from the misestimation of pension liabilities due to errors in the development, implementation, or usage of these models.	<u>Pension Risk Standard</u>
Climate Risk	Potential for loss and/or misstatement arising from the misestimation of climate risk due to errors in the development, implementation, or usage of these models.	<u>Climate Risk Standard</u>
Algorithmic Trading	Potential for loss and/or misstatement arising from the misestimation of algorithmic trading due to errors in the development, implementation, or usage of these models.	<u>Algorithm Trading models Standard</u>
Recommendation Systems	Potential for reputational risk and regulatory penalties due to bias when recommending products and services to consumers.	<u>Recommendation Systems Standard</u>

2.2 Geographies

Model RTF is rolled out at a Group level and formally adopted by Countries / Legal Entity / Markets, referred to as 'in-scope':

Europe & Americas: Germany and United States

Africa & Middle East: South Africa, UAE, Pakistan

Asia: China, Hong Kong, India, Malaysia, Singapore, South Korea, Taiwan, Thailand, and Vietnam

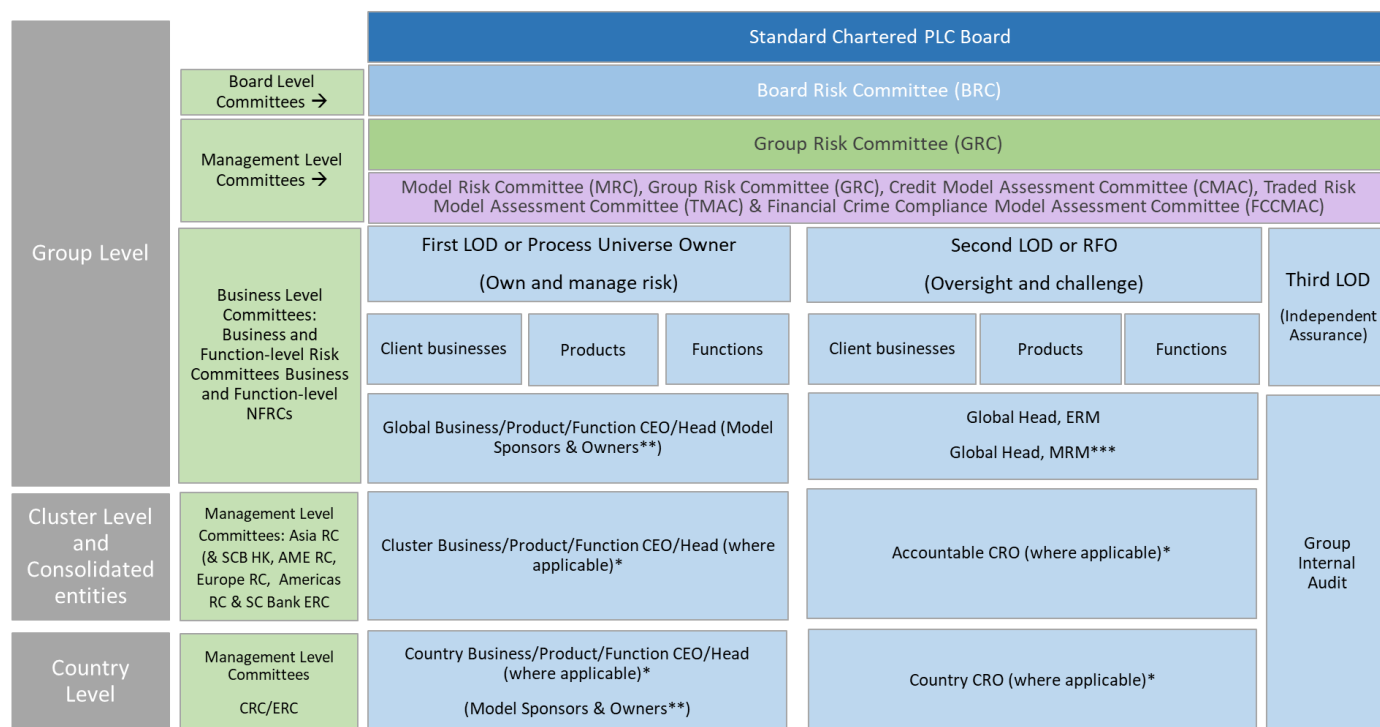
Legal Entity: SC Bank

There is no intent to cascade the framework to any further. CCROs of countries/entities/markets that are not in-scope can request to formally adopt the principles, if deemed necessary, by requesting approval from Model Risk, Group RFO.

3. Three LoD – Responsibility and Governance Committee Oversight

The Model Risk Framework reinforces clear accountability and roles for managing risk through the Three LoD model. The 1LoD is the business or function where the models are used and the model development function. **Model Risk Management (MRM)** – comprising **Group Model Validation (GMV)** and **Model Risk Policy and Governance (MRPG)** teams – forms the primary second line of defence function. The detailed set of Global, Cluster and rfo-level roles and responsibilities for the first and second line are provided in Figure 1 on the next page.

Figure 1: Model Risk – Overview of the Three Lines of Defence



* Please refer to Section 2.2 for list of countries that Model Risk as a PRT is applicable.

** Includes model identification, development, and monitoring teams where applicable.

*** Includes GMV and MRPG teams.

4. Decision making Authorities and Delegation

This chapter describes the formal mechanism through which the delegation of Model Risk authorities is made. The GCRO has delegated RFO authority to the Global Head, ERM as described in Section 1.1. The Global Head, ERM delegates authorities to designated individuals or policy owners through this Chapter, including second line ownership at a global business, product, and function level as well as cluster or country level.

The responsibility of oversight of effective roll out of the framework described in this chapter across the Group is delegated to the Global Head, Model Risk Management, with Country CROs responsible for branch or subsidiary compliance with the chapter.

5. Regulatory Obligations

5.1 Group-level Regulatory Obligations

The Global Head, ERM (or delegate) is responsible for ensuring second line oversight and challenge of legal and regulatory risks associated with their respective areas of responsibility, as covered by the following areas of regulations (non-exhaustive).

- Capital Requirements Regulations (EU) No. 575/2013 and related EBA Regulatory Technical Standards and Guidance.
- PRA Supervisory Statement 1/23 Model risk management principles for banks (effective from 17 May 2024).
- PRA Supervisory Statement 3/18 Model risk management principles for stress testing.

- Federal Reserve Supervisory Regulation 11/7 Supervisory Guidance on Model Risk Management for application to Standard Chartered Bank Limited, New York branch¹.

5.2 Breach and escalation mechanism

The Global Head, ERM or delegate is responsible for developing a breach and escalation mechanism for issues determined to be material by the RFO. Any breaches or potential breaches of relevant regulations must be escalated to the Global Head, MRM, Compliance function, as well as the business or function affected by the breach as applicable.

It is the responsibility of the Country CRO to notify the Global Head, MRM, Compliance function, and relevant business or function regarding any country level regulatory breaches or potential breaches leading to Model Risk. The Global Head, ERM or delegate should consolidate and escalate all such breaches to the MRC and any other relevant business and function-level Risk Committees and NFRCs, as necessary.

¹ While the Group Head, ERM or delegate is responsible for the model risk management framework, the US Country CRO or delegate is responsible for ensuring compliance of the New York branch with SR 11/7.

Appendices specific to this Framework

Appendix A: Version Control

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Zeeshan Arif	Initial version created as part of the consolidation of standalone RTFs during the ERMF/RTF simplification exercise.	Material	SC PLC Board	1.0	7 Dec 2023
Renzo Baio	Minor editorial change in section1.3, streamlining of language for clarity.	Non-Material	Jason Forrester	1.1	20 May 2024
Mark Green	Model Framework Updates towards New or Consolidated Group Standards, Model Families, Quantitative Methods definition with Models & DQMs	Non-Material	Jason Forrester	1.2	11 Dec 2024

Note: Please refer to Part C of the ERMF for common appendices.

----- END OF CHAPTER NINE -----

ENVIRONMENTAL, SOCIAL AND GOVERNANCE AND REPUTATIONAL RISK TYPE FRAMEWORK

Chapter Number	Ten – Part B of the ERMF
Principal Risk Type	Environmental, Social and Governance and Reputational Risk Type Framework
Risk Framework Owner Name	Jason Forrester
Risk Framework Owner Job Title	Global Head ERM & Deputy CRO SC Bank
Document Contact Name	Karen Wilkinson
Document Contact Job Title	Global Head, ESG and Reputational Risk
Version Number	2.0

Contents

1. Overview of the Environmental Social and Governance and Reputational Risk Type Framework3

1.1 Risk management principles3

1.2 Overview of ESGR Risk Framework4

2. Three Line of Defence Roles and Responsibility and Governance Committee Oversight4

3. Decision Making Authority and Delegation5

4. Regulatory Obligations and Escalation Mechanism6

4.1 Group-level Regulatory Obligations6

4.2 Country-level Regulatory Obligations6

4.3 Breach and Escalation Mechanism7

5. Risk Identification, Assessment, Monitoring, and Mitigation7

5.1 Risk Identification and Assessment7

5.2 Monitoring and Mitigation8

Appendices specific to this Framework9

Appendix A – Definitions9

Appendix B – Overview of Risk Management for ESG and Reputational Risks9

Appendix C – Links to Supporting Documents12

Appendix D – Version Control12

Version Control Table

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Vamshi Sa	RTF updated to include Climate risk within the existing Reputational and Sustainability risk RTF. The Reputational, Sustainability and Climate Risk is being merged into a single Principal Risk Type: "ESG and Reputational" (ESGR) Risk.	Material	Sadia Ricke	2.0	13 Dec 2024

The full version history is included in the RTF [Appendix D](#).

Chapter Ten

1. Overview of the Environmental Social and Governance and Reputational Risk Type Framework

1.1 Risk management principles

The **Environmental, Social and Governance** (ESG) and **Reputational Risk** (ESGR Risk) is defined as the risk of potential or actual adverse impact on the environment and/or society, the Group's financial performance, operations, or the Group's name, brand or standing, arising from environmental, social or governance factors, or as a result of the Group's actual or perceived actions or inactions. Additional definitions are in Appendix A.

The ESGR RTF (this Chapter) sets out the overall risk management approach for Reputational as well as ESG-related risk.

Below are the main principles that will form the basis of the ESGR Risk management:

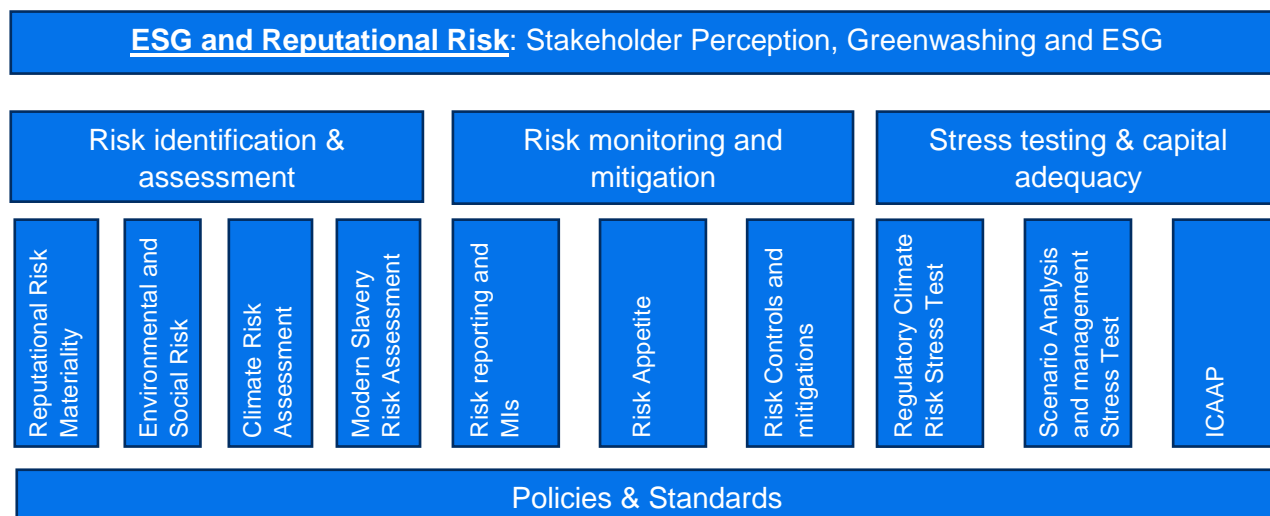
- The Group should uphold the principles of Responsible Business Conduct and continue to do the right thing for the stakeholders, the environment, and affected communities.
- The Group should adhere to its sustainability aspirations and public commitments and manage Greenwashing Risk arising from its sustainability-related statement, declaration, actions, or communications.
- Appropriate risk assessments should be taken to identify and assess ESG and Reputational risks for clients, transactions, product, projects, third party arrangements, and strategic decisions. Risk acceptances should be secured according to the Risk Acceptance Authorities.
- ESG and Reputational risks should be monitored on an ongoing basis and managed within Risk Appetite.
- Climate Risk can manifest through other **Principal Risk Types** (PRTs). The risk management requirements should be embedded in the respective RTFs, policies, and standards.

Of Environmental, Social and Governance categories, banks have historically focussed on Governance risk and therefore it has more mature risk management practices. For clients and third parties, Governance risk examples might include bribery, corruption, money laundering, tax evasion or corporate governance structure which for the Group are captured under the Compliance and Financial Crime Chapters. For the Group Operations functions, Governance risks include corporate governance and roles and responsibilities across the first, second and third LoD already governed through the Group's ERMF. Governance specific to management of **Environmental and Social** (E&S) risks is captured under the scope of this Chapter.

The Reputational Risk covered in this framework are the primary reputational risk that arises from the Group's strategic choices or decision on matters with apparent reputational risk at the time of decision making. Secondary reputational risk that is consequential (normally resulting from potential failure of another PRT), and does not occur at the point of decision-making, is outside the scope of this framework. Secondary reputational risk should be identified, assessed, and managed through the respective PRT RTFs using the **Group Risk Assessment Matrix** (GRAM) which incorporates key reputational risk considerations.

1.2 Overview of ESG Risk Framework

Figure 1: Overview of ESG Risk Framework

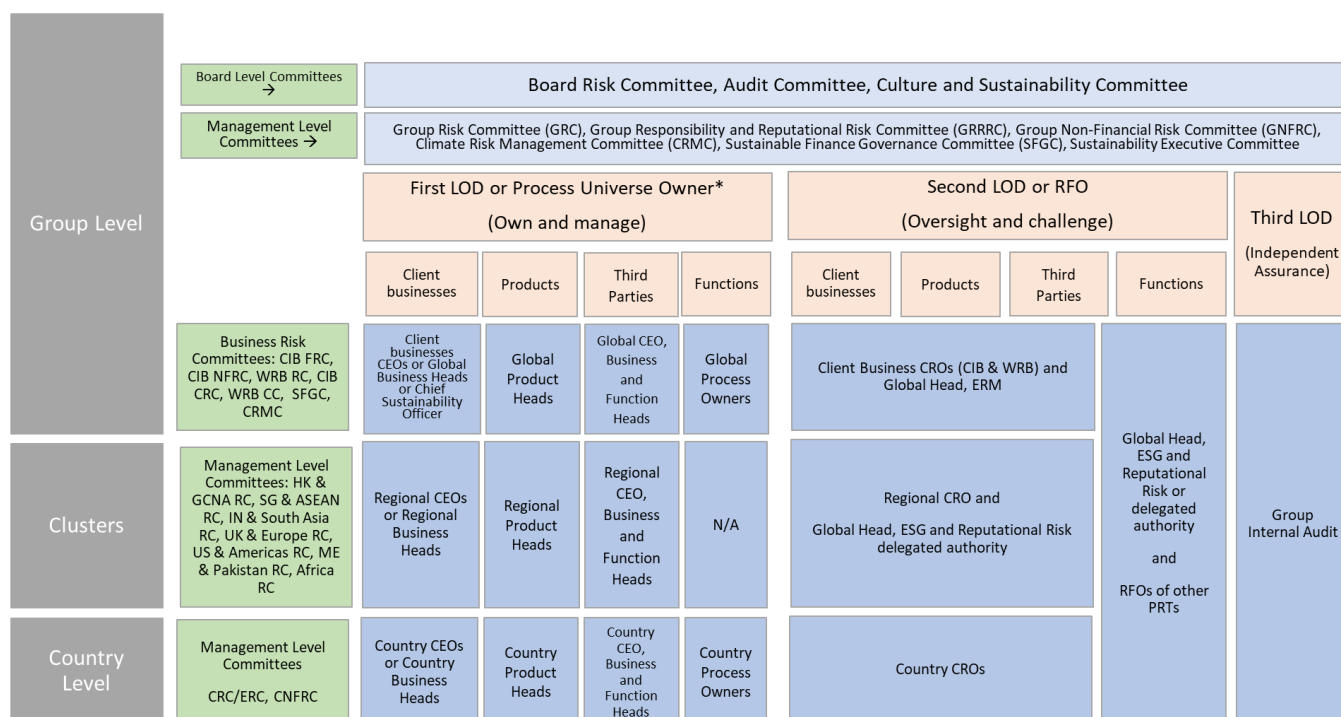


The overview of risk management for ESG and Reputational risks can be found in Appendix B.

2. Three Line of Defence Roles and Responsibility and Governance Committee Oversight

The ESGR RTF reinforces clear accountability and roles for managing risk through the three LoD model. A full overview of Global, Cluster and Country Level Governance committees that provide primary oversight for ESGR Risk are shown in the figure below.

Figure 2: ESGR Risk - Overview of the Three LoD and governance



At the local/country, clusters and global levels, the respective CEO, Business Heads, Product Heads and Function Heads are the first LoD of ESGR Risk. The first LoD complies with the applicable laws, regulations, and regulatory expectations and manages the risk that arises from first line activities.

Three Lines of Defence responsibilities are covered in ERMF Chapter 4. Additional specific responsibilities for First LoD are outlined below:

- **Client Businesses and Products:** Relationship Managers and deal team should consider Stakeholder Perception risk at the time of onboarding of the clients, provisioning of products, and should be monitored on an on-going basis for clients as set out in Reputational Risk Policy, ESG and Reputational Risk

Standard - CIB and ESG and Reputational Risk Standard - WRB. Relationship Managers must perform a client-level climate risk assessment. The **Environmental and Social Risk Management (ESRM)** team is a dedicated resource team supporting the management of E&S risks and impacts arising from the Group's client relationships and transactions. The team develops the Group's standards, supports clients to improve their social and environmental management practices, and identifies and mitigates risks for transactions and client relationships.

- **Third Parties:** Group Supply Chain Management owns the process for vendors and outsourcing arrangements and are a central function that leads the sourcing process for Businesses and Functions for vendor arrangements over set contract value and outsourcing arrangements. **Third Party Risk Management (TPRM)** is the second LoD for all vendors whereas ESG and Reputational Risk additionally oversees the E&S risks arising from third parties.
- **Functions:** All Functions that support the day-to-day operations of the Group are responsible for managing ESG and Reputational risks.

3. Decision Making Authority and Delegation

The ESGR RTF is the formal mechanism through which the delegation of ESGR authorities is made.

The Global Head, ERM delegates authorities to designated individuals or Policy Owners through this Risk Chapter, including second LoD ownership at a global business, product, and function level as well as cluster or country level. Authority is delegated to the Country CROs, Regional CROs, alongside the Global Head, ESG and Reputational Risk or delegate.

The Global Head, ERM delegates authorities to effectively implement this framework to the Global Head, ESG and Reputational Risk with the exceptions as below.

The Global Head, ERM retains authority and accountability for:

- Periodic reviews of this Chapter and approving non-material changes.
- Affirming Framework and Policy effectiveness to the GCRO.

Risk acceptances relating to the risk areas outlined in Table 3 must be secured prior to acceptance of any risks associated with potential or real negative shift in the stakeholder perception of the Group.

For example, a project financed in line with the Equator Principles may be subject to local stakeholder or NGO campaigns due to Environmental or Social risks. The Environmental or Social risks should be assessed prior to evaluation of Stakeholder Perception risk.

Table 3: Risk Acceptance Authorities

	Clients	Third Parties	Operations
Stakeholder Perception	For Clients, Medium risks may be accepted by Client Review Committees with ESGR Risk team as a quorum voting member. Group Responsibility and Reputational Risk Committee (GRRRC) has authority to accept High and Very High risks.	Risk Assessment to be done as part of RCSA.	
Greenwashing	<u>Sustainable Finance:</u> <ul style="list-style-type: none"> ▪ SF Labels are approved by Empowered Approvers. <u>Net Zero:</u> <ul style="list-style-type: none"> ▪ Clients that are misaligned with Net-Zero targets are monitored by Client Review Committees for setting action plans. 		
ESG	<u>ESRA:</u> <ul style="list-style-type: none"> ▪ Non-compliant ESRAs are approved by ESRM. 	<u>Modern Slavery:</u> <ul style="list-style-type: none"> ▪ ESGR Risk team as 2LoD accepts 	Risk Assessment to be done as part of RCSA.

	Clients	Third Parties	Operations
	<u>Climate Risk:</u> <ul style="list-style-type: none"> Black and Red graded CRAs are approved by Group ESGR Risk team. High climate risk clients without credible transition plan are monitored by Net Zero and Climate Risk Working Forum (NZCRWF). <u>Frameworks and Position Statements:</u> <ul style="list-style-type: none"> Frameworks¹ and Position Statements are approved by GRRRC. 	Modern Slavery related risks.	

Stakeholder Perception Risk for Digital Assets

Stakeholder Perception Risks associated with Digital Assets related projects or products or services which are assessed as Higher Risk as per 'Digital Asset Higher Risk Framework' are reviewed at **Digital Assets Risk Committee** (DRC) where ESG and Reputational Risk is a member, while Lower Risk DA initiatives follow existing BAU governance. Cases with High or Very High Stakeholder Perception risk ratings or cases where DRC deems to have material reputational concerns are escalated to GRRRC.

Stakeholder Perception Risk for Products

For Products, Global Head, ESG and Reputational Risk as the RFO delegate accepts ESGR Risks identified in **Product Programmes** (PPGs).

Stakeholder Perception Risk for Strategic Coverage Decisions

For Strategic Coverage Decisions, Global Head, ESG and Reputational Risk (or delegate) has the authority to accept Medium risks while GRRRC has authority to accept High risks.

4. Regulatory Obligations and Escalation Mechanism

4.1 Group-level Regulatory Obligations

The Global Head, ESG and Reputational Risk is responsible for second line oversight and ensuring compliance with the relevant regulatory obligations. The GRRRC will regularly monitor existing or new regulatory priorities.

For details on Policy and Standard Owners responsibilities in relation to Group-wide regulatory obligations, please refer to the ERMF.

4.2 Country-level Regulatory Obligations

For local regulatory obligations, the Local/Country CROs are responsible for identifying and maintaining oversight of emerging and existing ESGR related regulations. This includes ensuring the publication and obligation registers are up to date and escalating emerging ESGR Risk related regulations to the Group for central oversight. Local/Country CROs are responsible for end-to-end oversight of risk performance and should provide updates to Group ESGR Risk team where breaches or potential challenges in compliance are found².

¹ Environmental and Social Risk Management Framework, Green and Sustainable Product Framework, Sustainability Bond Framework and Transition Finance Frameworks

² The Target Operating Model for Group and Country horizon scanning process can be found [here](#)
ESG and Reputational Risk – Chapter 10

4.3 Breach and Escalation Mechanism

The Global Head, ESG and Reputational Risk is responsible for developing an appropriate breach and escalation mechanism for those breaches or issues determined to be material by the RFO. Escalation of breaches must be aligned with the response management requirements set out in the [Group Operational Risk Policy](#) and [Group Operational Risk Standard](#).

5. Risk Identification, Assessment, Monitoring, and Mitigation

5.1 Risk Identification and Assessment

5.1.1 Stakeholder Perception

At the point of decision-making impacting clients, transactions, products and strategic coverage, relevant processes as outlined in the Reputational Risk Policy must be used to assess Stakeholder Perception risk. Reputation Risk Materiality Assessment should be used to assess the materiality of stakeholder perception risks relating to clients and transactions across CIB and WRB.

The GRAM considers the negative shifts in perception of key stakeholder groups for the Group. Triggers are embedded within the first-line processes where Reputational Risk from a shift in stakeholder perception, through the failure of other PRT or at point of decision-making should be considered as part of RCSA.

Risks must be accepted according to the authority matrices set out in the [Reputational Risk Policy](#).

5.1.2 Greenwashing risks

The Group's Sustainable Finance portfolio must be assessed for Greenwashing risks and Process Owners for activities ensuring that SF labels are accurately applied and disclosed through the lifetime of the transactions should assess the risks and controls for Greenwashing risks part of RCSAs. Process Owners of various Functions in the Group must assess their processes for Greenwashing risks through the RCSA process.

5.1.3 ESG Risk

For Clients:

Triggers are embedded within the first-line processes where ESG risks including Climate risks should be considered. The **Environmental and Social Risk Assessment** (ESRA) is used to assess E&S risks by rating the level of alignment of the clients and transactions to the Group's Position Statements.

For Environmental Risk Indicator **Greenhouse Gas** (GHG) Emissions, an additional **Climate Risk Questionnaire** (CRQ) is used to assess the carbon intensity and transition abilities of the selected clients.

- Non-Compliant ESRAs must be accepted by ESRM prior to further risk acceptance.
- Black and Red graded Climate risk assessments must be accepted by ESG and Reputational Risk team.

In addition, to ensure that clients meet the Group's Position Statements, Regulatory Compliance Statements are established on a relationship level for CIB and certain WRB clients (Medium Enterprise). This Regulatory Compliance Statement outline the Group's expectations for clients on E&S risks and is issued to clients during onboarding.

For Third Parties:

A Modern Slavery Questionnaire is used to assess human rights and modern slavery risks for third parties.

For other E&S risks, the Supplier Charter sets out the Group's expectations for third parties to support and promote environmental protection, support, and respect the protection of human rights in accordance with the United Nation's Universal Declaration of Human Rights and UN Guiding Principles on Business and Human Rights. This is embedded in contractual clauses where possible.

Third-party continuity plans should include climate risk related disruptions. The Group is gathering material vendors operating site location data to assess their specific physical risk exposures, and to enhance third-party continuity plan where needed.

For Operations:

Process Owners of various Functions in the Group must assess their processes for risks relating to E&S through the RCSA process.

Climate Risk must be assessed for all existing and new properties and data centres using the tool maintained by the ESGR Risk team.

E&S Risk catalogue – A detailed classification of risk categories and risk indicators mapped to key industry guidance and the UN Guiding Principles in organizing the aspects of E&S risks that the Clients, Third parties and Operations must assess against. E&S Risk catalogue is available [here](#).

5.2 Monitoring and Mitigation

ESGR Risk is managed by maintaining a robust monitoring process that evaluate risk exposures across client, transactions, portfolio, third parties and own operations. The purpose of monitoring and mitigation is to provide ongoing oversight of activities and risk levels within the Group. Oversight is reinforced through structured processes, including risk sign-off, regular reporting, internal and external metrics, external media coverage and assurance processes.

On a periodic basis, updates are provided to the Group and Board Risk Committees on the ESGR Risk view of the portfolio.

In relation to countries, Country **Management Information** (MI) captures specific summary of key ESGR Risk parameters and risk appetite metrics. The MI aids country Chief Risk Officers in identifying country specific risk themes from underlying client data.

The comprehensive governance framework for monitoring and mitigation for ESGR Risk is meticulously outlined in the ESG Risk Policy and Reputational Risk Policy.

Appendices specific to this Framework

Appendix A – Definitions

Term	Definition
Environmental Risk	The potential material harm or degradation to the natural environment through the actions or inactions of the Group's operations, its clients, or third parties. If such risks eventuate, they may become adverse environmental impacts.
Social Risk	The potential to cause material harm to individuals or communities through the actions or inactions of the Group's operations, its clients or third parties. This includes aspects relating to labour and human rights. If such risks eventuate, they may become adverse social impacts.
Climate Risk	The potential for financial loss and non-financial detriments arising from climate change and society's response to it. It manifests through the Group's businesses and operations and impacts relevant Principal Risk Types (PRTs).

Appendix B – Overview of Risk Management for ESG and Reputational Risks

Stakeholder Perception (L3)	Clients	<ul style="list-style-type: none"> Stakeholder perception risk assessment for the clients and transactions must be assessed in accordance with Reputational Risk Materiality Assessment Matrix using the Reputational Risk Materiality Assessment (RRMA) form. At group level all products must be approved within the Product Programmes (PPG) and at country level all products must also be approved within a Country Addenda (CA) prior to marketing or transacting. For special interest industries with Stakeholder Perception Risk pertaining to other than environmental or social factors (for example, gambling or defence), the Group has Position Statements which articulate additional controls in place to manage or mitigate those risks. These must be approved by the Group Responsibility and Reputational Risk Committee (GRRRC).
	Operations	<ul style="list-style-type: none"> The Group manages Stakeholder Perception Risks associated with external communications and campaigns, media engagement, social media management and brand campaigns. Strategic coverage decisions (entry to new markets and sensitive industries and other strategic decisions) should be captured using Corporate Assessment Approval Form or the New Initiatives Consolidated Risk Assessment form, as relevant.

Greenwashing (L3)	Clients	<p>Sustainable Finance:</p> <ul style="list-style-type: none"> • SF-labelled (including transition portfolio) products, transactions and clients are deemed to be driving a positive E&S outcome for the stakeholders through holding the clients accountable to agreed Sustainability impact potential. These must be assessed for Greenwashing risks across labelling, transaction, client life cycle and disclosures to ensure potential positive impacts are assessed and reported fairly and negative impacts are not omitted. • Products and Transactions that carry a Sustainable Finance (SF) label are governed under the Green and Sustainable Product Framework. <p>Net Zero:</p> <ul style="list-style-type: none"> • The Group has net zero emissions targets relating to financed emissions, which is supported by reduction targets in key sectors. Science-based and sector-agreed methodologies are used to measure and govern the in-scope loan book to net zero. <p>Position Statements:</p> <ul style="list-style-type: none"> • Aligning the Position Statements to the Group's sustainability commitments helps to manage the risks of Greenwashing and address concerns regarding accusations of not achieving ESG targets quickly enough.
	Third Parties and Operations	<p>Commitments:</p> <ul style="list-style-type: none"> • The Group signs on to several commitments that are aligned to the overall strategy impacting businesses, supply chain and operations. Taking responsibility over the tracking and realisation of these commitments helps to manage allegations of Greenwashing. • The risk of not adhering to the Group's Sustainability aspirations is managed by ensuring that the Group signs up to commitments that is aligned to its overall strategy and monitors ongoing progress. <p>Net Zero:</p> <ul style="list-style-type: none"> • The Group has targets in place to become Net Zero (Scope 1 and Scope 2) in its own operations by 2025. <p>Disclosures:</p> <ul style="list-style-type: none"> • Greenwashing considerations are implicitly linked to accurate disclosures which is managed by Finance via principles laid out in financial reporting policies that govern the Group's disclosures in making sure that they are fair, balanced, and understandable. <p>Campaigns:</p> <ul style="list-style-type: none"> • Greenwashing risks can also be triggered from external campaigns related to sustainability themes or SF products. All sustainability-related product marketing campaigns and communications should engage Corporate Affairs, Brand and Marketing (CABM) team and apply respective CABM Communication standards and Standards for Segment Campaigns set globally and locally.

ESG (L3)	Clients	<p>Position Statements:</p> <ul style="list-style-type: none"> • The Group articulates its management of E&S risk relating to clients through detailed Position Statements and a Prohibited Activities List. These are reviewed periodically in order to evolve with international good practice. • The Group's Position Statements are incorporated into the Regulatory Compliance Statement which is provided to clients at onboarding and is applicable on a relationship level. • Clients operating in sensitive sectors are expected to meet the standards outlined in the Position Statements, which is verified by the E&S Risk Assessment. Where clients are non-compliant with this or show insufficient progress with timebound action plans, the Group will decline transactions or seek to exit client relationships subject to contractual provisions <p>Equator Principles:</p> <ul style="list-style-type: none"> • The Group will not provide financing or advisory services to Projects to which the Equator Principles apply where the borrower will not or is unable to comply with the principles. <p>Climate Risk:</p> <ul style="list-style-type: none"> • The Group manages financial and non-financial risks arises from climate change both at an individual client and portfolio level. • Climate Risk Assessment is integrated within Business Credit Application process. Climate Risk Questionnaire is used to identify, assess, manage and monitor the climate related risks within credit risk.
	Third Parties and Operations	<ul style="list-style-type: none"> • The Supplier Charter sets out the Group's expectations on human rights, environment, health and safety standards, labour, and protecting the environment. Relevant clause is included in supplier contracts where possible. • Suppliers should be assessed for Modern Slavery and human rights related risks at onboarding and over time through adverse media screening. • The Group maintains a list of Goods and Services and Countries with high risk for Modern Slavery. • The Group commits to minimize its impact on the environment and have targets in place to reduce its carbon, energy, water, and waste. • The Group manages social risks within its own operations through a variety of approaches under the responsibility and remit of CABM, Human Resources and Operational, Technology and Cyber Risk. • The Group identifies climate related risks within its businesses and functions. • Climate Risk must be assessed for all existing and new properties and data centres using the tool maintained by the ESGR Risk team. • Third-party continuity plans should include climate risk related disruptions.

Appendix C – Links to Supporting Documents

Please visit the ESG and Reputational Risk [SharePoint page](#) to find the following documents:

- Reputational Risk Materiality Assessment Matrix
- E&S Risk Catalogue

Appendix D – Version Control

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Zeeshan Arif	Initial version created as part of the consolidation of standalone RTFs during the ERMF/RTF simplification exercise.	Material	SC PLC Board	1.0	7 Dec 2023
Renzo Baio	<ul style="list-style-type: none"> • Refreshed the Reputational and Sustainability Risk (RSR) RTF chapter to reflect some factual changes and updates. • Section 1.1: Added definitions of Environmental and Social risk in alignment with E&S framework. • Section 1.1.1: Deleted reference to Summaries of Approach as they are replaced by Position Statements and added 'Greenwashing risk'. • Section 1.1.2 (Environmental and Social Risks): Updated review frequency of Position statements to periodic from every two years. Minor edits to clarify 'Supplier Charter' to reflect only areas of oversight for ESGR Risk. Included screening criteria for human-rights related risks. • Section 2: Added First LoD responsibilities of considering Stakeholder Perception risk at the time of onboarding of clients and an ongoing basis for in-scope clients. • Section 3: Added risk acceptance authorities for Products and Strategic Coverage Decisions. <p>ERMF Part C: Minor Updates to list of priority reports</p>	Non-Material	Jason Forrester	1.1	28 May 2024
Vamshi Sa	RTF updated to include Climate risk within the existing Reputational and Sustainability risk RTF. The Reputational, Sustainability and Climate Risk is being merged into a single Principal Risk Type: "ESG and Reputational" (ESGR) Risk.	Material	Sadia Ricke	2.0	13 Dec 2024

Note: Please refer to Part C of the ERMF for common appendices.

----- END OF CHAPTER TEN -----

INFORMATION & CYBER SECURITY RISK TYPE FRAMEWORK

Chapter Number	Eleven – Part B of the ERMF
Principal Risk Type	Information and Cyber Security
Risk Framework Owner Name	Adrian Munday
Risk Framework Owner Job Title	Global Head, Operational, Technology and Cyber Risk
Document Contact Name	Marek Kwas
Document Contact Job Title	Director, OTCR, ICS Framework
Version Number	2.0

Contents

1. Overview of the ICS Risk Type Framework.....3

1.1 ICS Risk Management principles3

1.2 Overview of ICS Risk Governance Model4

2. Three LoD Responsibility and Governance Committee Oversight.....4

3. Decision Making Authority and Delegation5

4. Regulatory Obligations and Escalation Mechanism.....5

4.1. Group-level Regulatory Obligations5

4.2. Country-level Regulatory Obligations.....6

5. Risk Identification, Assessment, Monitoring and Mitigation7

5.1 ICS Risk Identification and Assessment.....8

5.2 ICS Risk Treatment (Mitigation)8

5.3 ICS Risk Monitoring & Reporting8

Appendices Specific to this Framework9

Appendix A: ICS Risk Management Activities.....9

Appendix B: ICS Policies15

Appendix C: Version Control.....16

Version Control Table

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Maker Kwas/ Anita Madro	<ul style="list-style-type: none">ICS Risk Management Principles reviewRefresh of the Overview of ICS Risk FrameworkAlignment of the ICS Framework to OTCR modelUpdated Risk management requirements incorporated into Appendix A	Material	Sadia Ricke	2.0	13 Dec 2024

The full version history is included in the RTF [Appendix C](#).

Chapter Eleven

1. Overview of the ICS Risk Type Framework

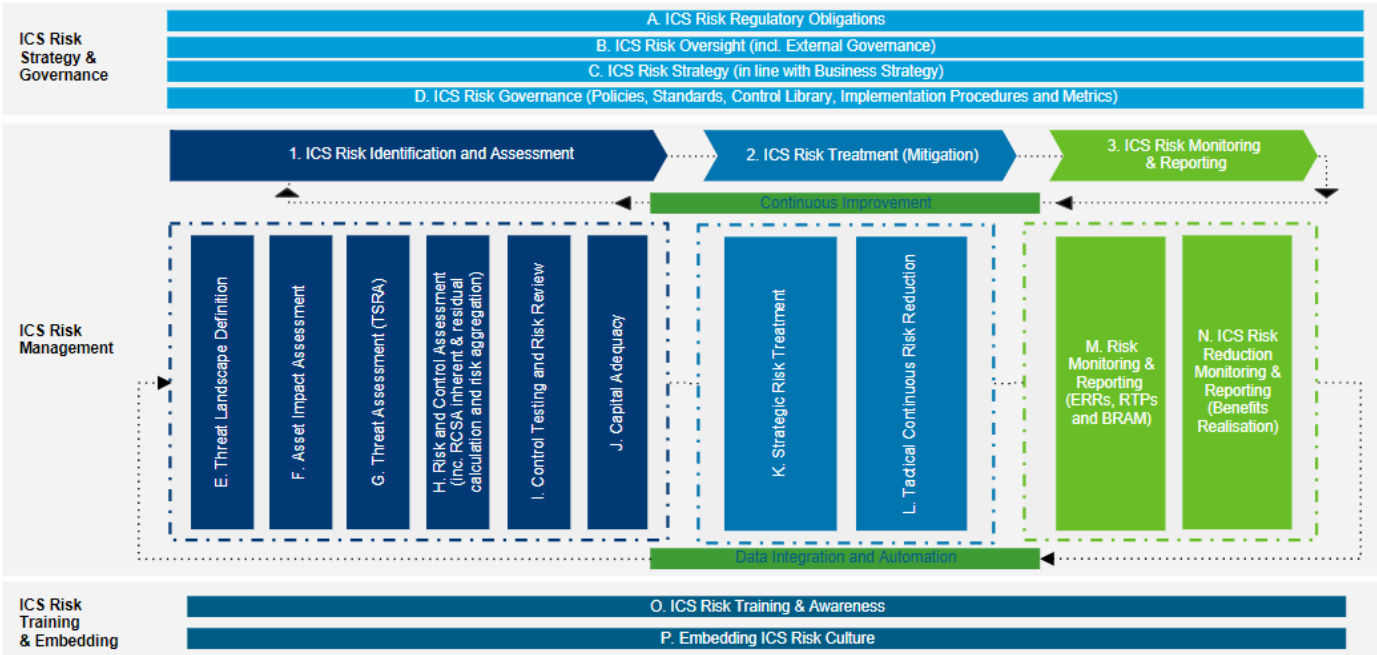
The **Information and Cyber Security** (ICS) RTF (this Chapter) outlines the areas of governance and risk management approach unique to the PRT.

1.1 ICS Risk Management principles

- Board and executives engage to drive a culture of security excellence and robust governance of control effectiveness.
- Businesses are accountable for the identification and management of ICS risk.
- Embed security and resilience by design, automating processes to drive efficiency where possible.
- Embed security at each stage of client journeys to protect the Group's and our Clients' Information Assets, Information Systems, supporting Technology Infrastructure and services, including the ones supported by Third Parties.
- ICS risk is managed using a **Threat Scenario led Risk Assessment** (TSRA) approach. The Group's Information Assets and Systems are assessed in the context of their criticality and of the threats the assets are exposed to. Adequate risk treatment is applied to identified material risks.
- Group Information Assets, Systems and Technology Infrastructure should be secured in compliance with applicable ICS Policy and Standards.
- Embed proactive management of risk through horizon scanning for potential threats and control gaps and manage identified control weaknesses.
- Embed a healthy culture across our staff to proactively manage ICS risk through the shared responsibility to defend against threats, continuous improvement and transparent risk decision making. This will build trust and drive sustainable value for our stakeholders.
- Ensure staff are adequately trained to securely use Information Assets, Systems and Technology Infrastructure and monitor their usage to detect and report potential security incidents.
- Third Parties who use, or process Group Information Assets, Systems or Technology Infrastructure must comply with Policy and applicable Standards.
- Incidents affecting the Group's Information Assets, Information Systems, or Technology Infrastructure are identified and managed to minimize their impact, and
- Lessons learnt from past ICS incidents and risk mitigations are incorporated into future risk management plans.

1.2 Overview of ICS Risk Governance Model

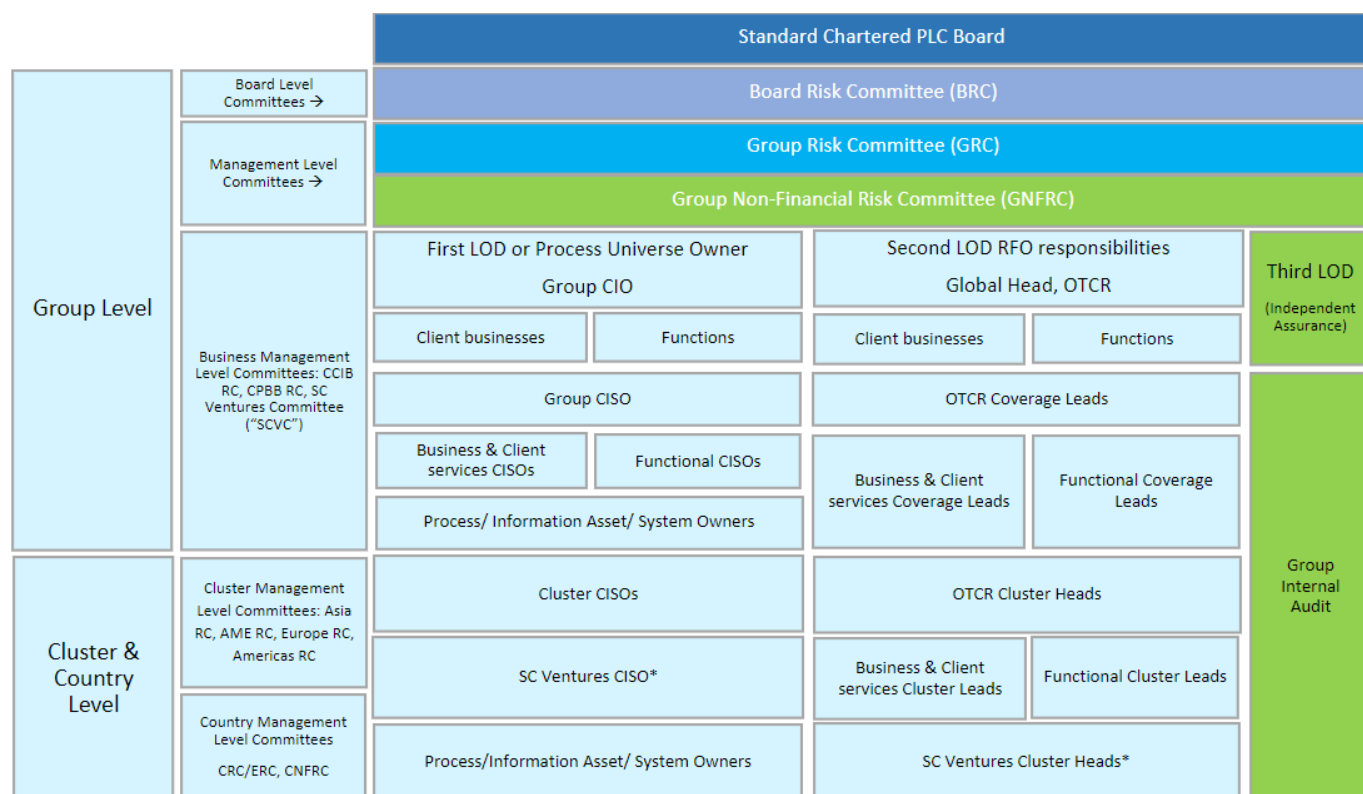
Figure 1: Overview of the ICS Risk Framework



A description of the End-To-End Risk Management and Governance activities can be found in the Appendix A

2. Three LoD Responsibility and Governance Committee Oversight

- 2.1. The first LoD (1LoD) are the businesses and functions that own and manage Information Assets, Information Systems, Applications and Technology Infrastructure. Overall responsibility for 1LoD of ICS Risk resides with the **Group Chief Information Officer (GCIO)** The development and execution of the ICS strategy is led by the **Group Chief Information Security Officer (CISO)** who has delegated authority from the Group CIO. The ICS RTF assigns specific responsibilities for 1LoD management of ICS to Information Asset Owners, Information System Owners, Application Owners, Technology Infrastructure Owners, and Process Owners. For more information on the obligations of specific role holders please refer to the ICS Policy.
- 2.2. The **Operational, Technology and Cyber Risk (OTCR)** function within the Risk Department is the second LoD (2LoD) and provides independent challenge, guidance, and oversight of 1LoD risk management. The OTCR function is led by the Global Head, Operational, Technology and Cyber Risk, who has delegated authority from the GCRO.
- The OTCR function comprises of OTCR ICS Framework, OTCR Business / Function Coverage Leads and OTCR SMEs who support the Global Head, OTCR. The OTCR sets the methodology for assessing, and prioritising ICS risks across the Group. Risk Management authorities for ICS Risks are executed in line with the Appendix D – Risk Acceptance and Treatment Plan Escalation, Approval and Closure Authorities defined in the Group Operational Risk Standard.
- 2.3. Audit acts as the third LoD (3LoD), independently assessing whether 1LoD and 2LoD controls and risk management processes are effective as outlined in Part A of the ERMF.
- 2.4. The detailed set of Global, Cluster and Country-level roles for the 1LoD and 2LoD are provided in Figure 2 below. Additional information on roles and responsibilities can be found in the ICS End to End Risk Management & Governance RACI (ICS E2E RM&G RACI) available on [One Stop Shop \(sharepoint.com\)](#).

Figure 2: ICS - Overview of the Three Lines of Defence¹

*Type A ventures report in the same manner as businesses and countries. Type B ventures report up into country/regional risk committees, while Type C and D ventures report into SC Ventures Committee, which reports up to GRC.

3. Decision Making Authority and Delegation

- 3.1. Through this chapter, the formal delegation of ICS authorities is made. The Global Head, OTCR delegates authority to designated individuals or Policy Owner including 2LoD ownership at a global business and function level as well at cluster and/or country levels. Further details of the policy delegation have been included in section 4.1 of the ICS Policy.
- 3.2. Where delegation is required, the named role remains accountable and must be able to assure the appropriateness of delegated authority. At a minimum this includes appropriate ICS skills, segregation of duties and non-sharing of credentials. Where delegated activity requires seniority level to be retained, seniority requirements must be defined within activity definition.

4. Regulatory Obligations and Escalation Mechanism

4.1. Group-level Regulatory Obligations

The Global Head, OTCR (or delegate / SME) is responsible for ensuring 2LoD oversight and challenge of legal and regulatory obligations associated with PRA - Operational Risk and Operational Risk Rules.

For regulations, issued by Financial Services Regulators, Compliance will identify new and amended regulations as and when issued and communicate the relevant regulatory obligations to the applicable RFO delegate / SME.

The Global Head, OTCR is responsible for:

- identifying and documenting all the ICS related regulations, to be applied group-wide for this RTF.
- identifying regulatory authorities in all countries where the Group operates, who may issue regulations relevant to the Group for the areas of regulations within the RTF.
- identifying material regulations relevant to the Group issued by those regulatory authorities.
- publishing policies and standards covering the requirements of the relevant regulatory obligations.
- overseeing and monitoring implementation of those policies and standards.
- maintaining adequate traceability to demonstrate material regulations have been identified linked to policies and standards and communicated to 1LoD for implementation.
- providing 2LoD oversight and challenge of the compliance risk as relevant to their RTF and controls identified.
- oversee attestations to regulatory authorities to confirm compliance to the relevant regulations, in-line with Section 14 of the ERMF.

The Group CISO is responsible for:

- notifying Global Head, OTCR as and when they become aware of any regulations relevant to ICS issued by non-financial services regulatory authorities.
- identifying the relevant Process Owners responsible for implementing the regulation in their processes and informing Global Head, OTCR.
- implementing ICS Policy and Standards.
- ensuring mechanisms are in place to demonstrate that necessary documentation and audit trail concerning implementation of ICS **Legal Regulatory and Mandatory** (LRM) requirements are maintained.
- provide required inputs for supporting the completion of attestations to relevant regulatory authorities to confirm compliance towards the relevant regulations.
- tracking remediation of gaps identified from LRM attestations in line with remediation programmes.

4.2. Country-level Regulatory Obligations

Regulatory obligations to be implemented at a local/country-level may emanate from both **Extraterritorial Regulation** (ETRs) and local regulatory authorities.

The Country RFO is the Country Operational, Technology and Cyber Risk Head, (Country OTCR Head).

The responsibilities for the various stages of the regulatory lifecycle are specified in Table 1 below.

Table 1: Regulatory lifecycle in countries

Activity	Responsibility in country
Identify material relevant regulatory authorities on an on-going basis	Country RFO
Ensure completeness of regulatory authorities and ownership	Country CEO exercised through CNFRC
Ensure the identification of material new and amended laws and regulations issued by Financial Services Regulatory Authorities as and when issued	Country Head of Compliance
Ensure the identification of relevant new and amended laws and regulations issued by sources other than financial services regulators as and when issued	Country RFO delegate or SME
Ensure all necessary documentation and audit trail exists for laws and regulations to demonstrate the process from identification through risk assessment, applicability assessment, dissemination to	Country RFO delegate or SME

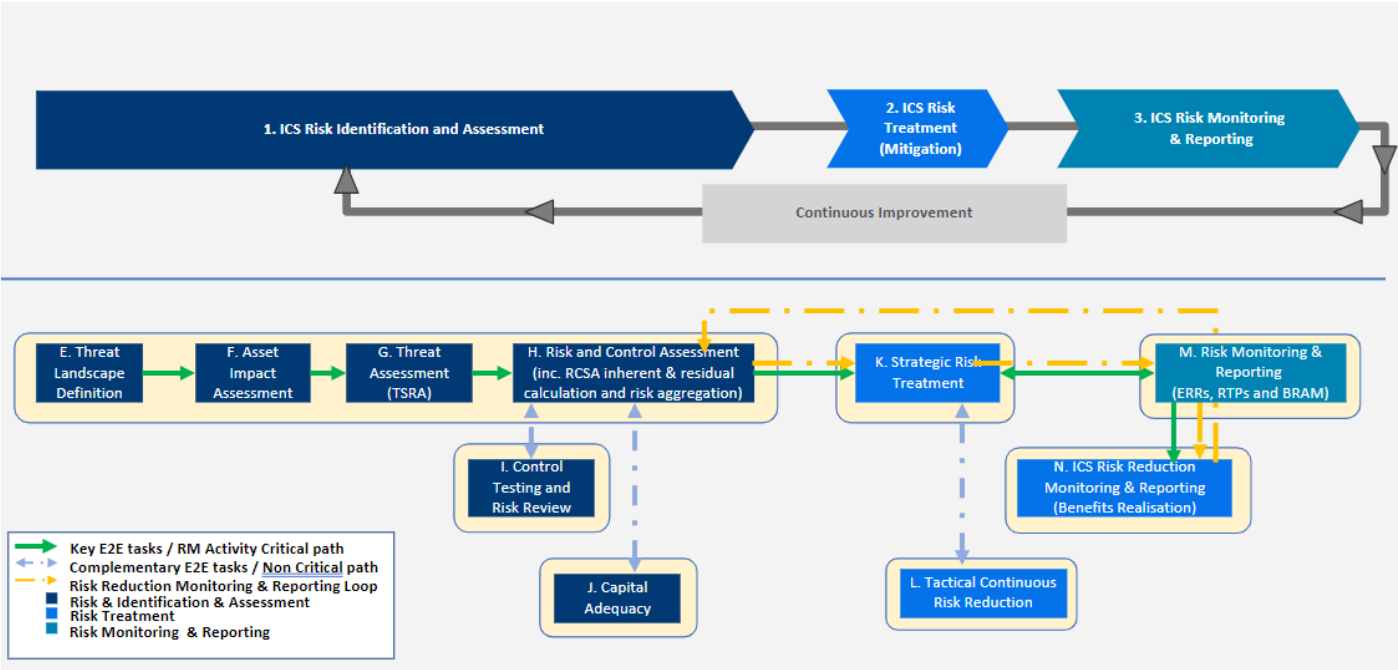
Activity	Responsibility in country
relevant first line and to confirmation of implementation by the relevant first line.	
Second line oversight and challenge of the risks and controls identified	Country RFO delegate or SME
Adherence to regulatory requirements as defined within ICS Policy and Standards, as defined by OTCR and Compliance and as per local laws and regulations.	Country CEO
Identify and communicate to Country OTCR Head all required local variations to ICS RTF or ICS Policy.	Country CISO with the approval from Country CEO
This should be captured in the Local Addendum document.	Country RFO and Country Head of Compliance.

5. Risk Identification, Assessment, Monitoring and Mitigation

The Global Head OTCR sets the overall methodology for assessing ICS Risk across the Group with the use of the **Threat Scenario-led Risk Assessment** (TSRA) methodology aligned to the Group’s RCSA approach. This methodology aims to provide guidance to support the production of operational processes to deliver a standardized and repeatable way of assessing ICS risks in alignment with Group RCSA process, proactively considering threats to the Group’s Information Assets and Systems as part of this Risk Assessment.

The ICS Policy and Standards define control requirements for the management of ICS Risk by the 1LoD. Global Head, OTCR delegates development and maintenance of the ICS Standards to Group CISO.

Figure 3: ICS Risk Management Components



5.1 ICS Risk Identification and Assessment

ICS Risk Identification and Assessment is the first of three sub-components that make up the ICS Risk Management section of the Framework. Its primary purpose is to identify ICS threats that are relevant to the Group, assess their inherent risk (impact and likelihood), and how effective the Group's controls are at mitigating them (residual risk).

The detailed table of dynamic risk identification process, along with other ICS risk management activities can be found in Appendix [A]. Additional details for the roles and responsibilities are provided in the ICS E2E RM&G RACI available on [One Stop Shop \(sharepoint.com\)](#).

5.2 ICS Risk Treatment (Mitigation)

ICS Risk Treatment is the second sub-component within the ICS Risk Management. Risk treatment aims to reduce the impact and likelihood of identified risks back within the Group's appetite through the application of strategic, tactical, and operational measures. Risks can be managed through reduction, acceptance, avoidance, or transference.

5.3 ICS Risk Monitoring & Reporting

ICS Risk Monitoring & Reporting is the third sub-component of the ICS Risk Management. Its purpose is to continuously monitor ICS risks against appetite and risk objectives, and to report the Group's current ICS risk posture, and the benefits delivered through improvement activities.

Description of the ICS Risk Management activities listed here is provided within the [Appendix A](#). The output of the above processes is communicated by the Global Head, OTCR to the ERM Forum on a quarterly basis.

Appendices Specific to this Framework

Appendix A: ICS Risk Management Activities

Activity/Process	Sub-activity Index	Sub Activity Name	Sub Activity Description
A. ICS Risk Regulatory Obligations	A1.	ICS Risk Regulatory Obligations	Identify, document, and maintain ICS regulatory requirements. The ICS Legal Regulatory and Mandatory (LRM) Obligations Register and the ICS Policy / Standards Gap Analysis must be reviewed and updated at least on an annual basis, or upon the mandate of a new or modified LRM requirement applicable to the Bank and the relevant markets and countries it operates within.
	A2.	ICS RTF Local Addendum (including ICS Policy Addendum)	Identify, document, and approve country-specific regulatory demand or material variations to the Group ICS Risk Type Framework and/or ICS policy.
	A3.	ICS Risk Regulatory Attestations	Design an Operating effectiveness review of the Bank's controls against regulatory obligations prior to submission to regulators.
B. ICS Risk Oversight (incl. External Governance)	B1.	Set Annual ICS Risk Appetite	A methodology providing guidance, approach, and responsibilities on the setting of risk appetite for Group, SC Bank, SOLO and Entity Risk Appetite Allocation (ERAA) Countries, including the definition and refresh of requirements for the ICS Board Risk Appetite Metrics (BRAM).
	B2.	ICS Risk Oversight	OTCR Coverage teams in consultation with ICS SME team (where required), on behalf of the RFO, provides oversight and governance of key ICS Risk activities across the Group. This includes oversight of ICS Risk papers, ICS Risk profiles and Board Risk Appetite. In addition, oversight is also performed by risk committees as defined by the ICS RTF and their respective Terms of Reference (ToR), including Board Risk Committee (BRC), Group Risk Committee (GRC), Group Non-Financial Risk Committee (GNFRC) and Business/Function Non-Financial Risk Committees (NFRC)
	B3.	OTCR Risk Reporting Requirements	Evaluation of the Group's data and reporting capabilities (infrastructure & tooling) that are required to support the ICS Risk Appetite Reporting and assessed against the Basel Committee on Banking Supervision (BCBS) 239 principles for Data Aggregation & Reporting.

Activity/Process	Sub-activity Index	Sub Activity Name	Sub Activity Description
	B4.	Third Party Security Risk Oversight	Establish baselines and policies to manage Third Party Security risks; guidance on what good looks like, and monitor activities to identify trends and cases where risk tolerances may be breached.
C. ICS Risk Strategy	C1.	Define ICS Strategy (CISO)	The first line of defence (1LoD) ICS Strategy (CISO) must be defined and supported by the ICS Strategic Journey that outlines how long-term security outcomes are delivered including timelines for increasing security maturity.
D. ICS Risk Governance	D1.	ICS Risk Type Framework	Group Information and Cyber Security Risk Type Framework (ICS RTF) must document at a high-level risk management principles, risk sub-types, risk appetite (RA), second line processes for oversight and challenge, key first and second line roles and responsibilities, decision making authorises, delegation of authority, regulatory obligations and approach to risk assessment, identification, and monitoring against RA.
	D2.	ICS Policy	The Group ICS Policy is a set of internal rules and principles that are established to help the Group to adhere to external or internal requirements. The Group ICS Policy is part of ICS risk framework that guides in decision-making, process design and desired behaviour through policy statements.
	D3.	ICS Standards	The development and maintenance of controls documentation to define the minimum control requirements that align to industry standards and core market regulations. ICS Standards support higher level statements in the ICS Policy.
	D4.	ICS Methodologies	ICS Methodologies are a high-level description of 'how to principles' to support implementation of the Framework, Policy, or Standards. The ICS Methodologies must be reviewed according to the frequency set out by the ERMF, considering the guidance and requirements set out by the ICS RTF.
	D5.	Controls Library (including Metrics Definition)	Consolidation and maintenance of single repository of all ICS-relevant Process Controls and Metrics from TTO RCSA Processes, Business / Functions TSRA and Control Testing. Provide a view of ICS Controls mapped to ICS Standards
	D6.	ICS RTF Effectiveness Review	The Group Risk Framework Owners ('RFO') and Group Policy Owners must affirm the effectiveness of the RTFs and Policies through an evidence-based attestations approach. The RTFs and Policies set out the approach for conducting Effectiveness Reviews. The approach is additionally supported with evidence acquired through the Risk and Control Self-Assessments ("RCSA") and other oversight/challenge governance activities.

Activity/Process	Sub-activity Index	Sub Activity Name	Sub Activity Description
	D7.	Enterprise Security Architecture	<ul style="list-style-type: none"> Align Enterprise Security Architecture to business strategies. Support development of strategic cyber security capabilities for the Bank. Navigate threats, regulatory, and ICS control landscape to prepare the Bank for future security needs. Communicate the principles for how we build and govern security capabilities in the Bank. Develop the necessary processes, tooling, and governance to ensure Security Architecture is embedded throughout the organization's Enterprise Architecture practices. Develop security related non-functional requirements for platforms and other technology infrastructures, applications, products, and service integrations.
	D8.	ICS Metrics Publishing (including development where applicable)	ICS Metrics required for the Threat Scenario Risk Assessment (TSRA) must be published on Sentinel as per the agreed metric frequency. The Board Risk Appetite Metrics (BRAM) must be published monthly on the BRAM dashboards within the Sentinel tool. Where metrics are applicable to be developed and automated, this activity is done by the ICS R&G team.
E. Threat Landscape	E1.	Identify Threat Landscape	The Cyber Intelligence Centre (CIC) serves as the intelligence hub, collecting intelligence from a variety of sources and providing threat analysis capabilities to a broad range of internal stakeholders, from operational teams through to executive management.
F. Asset Impact Assessment	F1.	Technology Lifecycle and Configuration Management	The process governs the Technology Products, Technology Assets (including Licensing and Obsolescence), Configuration Items as well as the Monitoring and Reporting Management for overall Technology Lifecycle Management.
	F2.	Information Asset and S-BIA	The Information Asset Owners/System Owners are required to use the Impact Assessment criteria to assess the value of their Information Asset/System to the Group. This value is the impact to the Group if the information is lost or compromised from a Cyber Security point of view. An overall rating is calculated using the Inputs from the Information Asset Owner/System Owner. Confidentiality, Integrity and Availability impacts must be assessed using the GRAM and a rating assigned to each criterion.

Activity/Process	Sub-activity Index	Sub Activity Name	Sub Activity Description
	F3.	Asses Third Party Risk Exposure	The TPSA process is a security risk assessment, aimed at determining ICS Risk and assessing the Information and Cyber Security (ICS) control environment of external Third Parties that have access to the Bank's non-public information, and/or access or host systems that process such information. The process is performed during the onboarding of the Third Parties or on an ongoing basis (under a predefined period).
	F4.	Cyber Attack Surface	The Attack Surface reports the change in size of the organization by asset type (People, Providers, Connectivity, System and Data) encompassing indicators, which represent the known exposure to threats. It aims to provide awareness and visibility to drive high-value, strategic conversations for business decision-makers by utilizing the information to reduce the size and complexity of asset types.
G. Threat Assessment TSRA	G1.	Define Threat Scenarios	Define the threat scenarios most relevant to the organisation based on an assessment of who is likely to target it and why.
	G2.	Assess Inherent Risk	The inherent risk (impact and likelihood) of applicable ICS risk category / Threat Scenario is assessed based on the understanding of business context, associated assets and its attack surface, supported by analysis of real-world incidents in terms of proximity, prevalence, and sophistication. The inherent risk is assessed in line with the frequency defined by Group RCSA framework
	G3.	Report Threat Exposure	Report on the number of incidents of different types (inc. near misses), learnings from external and internal incidents and developments in the threat landscape using data visualisation and dashboards.
	G4.	Map Controls to Threat Scenarios	Identify and map which controls are key in helping to prevent, detect or correct relevant threat scenarios/ vectors across the stages of the cyber-attack kill chain.
H. Risk and Control Assessment TSRA	H1.	Risk and Control Assessment	Any ICS risk identified must be assessed using the Group's Risk Assessment Matrix. The ICS risk assessment must determine the inherent risk rating, assess mitigating controls, and determine the residual risk rating. The residual rating determination is supported by the effectiveness and coverage analysis of ICS controls for applicable risks/threats and considers risk reduction afforded by key controls to detect, protect, respond and recover from an ICS threat/risk. The inherent

Activity/Process	Sub-activity Index	Sub Activity Name	Sub Activity Description
			and residual risks are assessed in line with the frequency defined by Group's RCSA framework.
	H2.	Cyber and Technology Emerging Risk Management	Identify, assess and prioritise emerging Cyber and Technology risks, working with partners and stakeholders to facilitate the proactive management of horizon risks.
I. Control Testing and Risk Review	I1.	ICS Control Testing	ICS (Information Cyber Security) Control Testing is intended to assess both the design adequacy and operating effectiveness of ICS controls listed and maintained in the ICS M7 Controls Library. ICS controls must be implemented to manage the risk Across the ICS Risk Type Framework (ICS RTF) which underpin the business risks, as defined in the group-wide Operational Risk Type Framework (ORTF).
	I2.	Third Party Security Assessment TPSA	The TPSA process is a security risk assessment, aimed at assessing the Information and Cyber Security (ICS) control environment of external Third Parties that have access to the Bank's non-public information, and/or access or host systems that process such information. The process is performed during the onboarding of the Third Parties or on an ongoing basis (under a predefined period)
	I3.	OTCR Assurance & Testing	Conduct risk-focused, evidence-based independent assessments to assess the design and operating effectiveness of controls. Key Methodology: The Second Line Assurance (2LA) Methodology.
	I4.	Red Teaming	Red Team Operations are risk based, intelligence led, scenario driven assessments that simulate the actions of real-world cyber adversaries targeting the organisation. The goal is to assess the capability of the Bank to prevent, detect and respond to a cyber-attack targeting critical Lines of Defence through compromise of key systems, data, and people. The exercises do this by simulating and emulating the actions and methodologies of real-world adversaries with the same level of intent, sophistication and capability as well as providing scenarios with new techniques, that potentially could be used by attackers. In doing so, the exercises can help identify weaknesses that traditional cyber security testing may not find.
J. Capital Adequacy	J1.	Capital Adequacy	This activity identifies the Group's capital adequacy requirements as they relate to ICS risk i.e., the threat scenarios that should be modelled to support capital adequacy planning.
K. Strategic Risk Treatment	K1.	Define Risk Treatment Plan	Risk Treatment Plans are strategic plans of activities which must be defined to help reduce elevated residual risks, so they are within the risk appetite of the organisation, taking organisational and budgetary constraints into consideration.

Activity/Process	Sub-activity Index	Sub Activity Name	Sub Activity Description
			Treatment Plans for their respective Elevated Residual Risks must be defined and reviewed according to the guidance and requirements set out by the Group Operational Risk Standard.
	K2.	ICS Dispensations	A dispensation must be obtained if any of the requirements mandated in the Group Information and Cyber Security Policy (GICSP) or related ICS standards cannot be met, resulting in Medium or above risk (in GRAM) and an explicit decision is taken not to remediate. Where possible risks should be remediated, and Dispensations will only be approved for exceptional cases.
L. Tactical Continuous Risk Reduction	L1.	Purple Teaming	The goal of the Purple Team is to conduct adversarial simulations (i.e., emulating realistic threat actors) by carrying out intelligence-informed attack scenarios with maximized defense team interaction to continuously improve prevention, detection and response capabilities, in a controlled manner.
M. Risk Monitoring and Reporting	M1.	Risk Monitoring	ICS risk must be monitored on a regular basis to demonstrate to 2LoD, Senior Management and Board that ICS control performance, and its potential impact on organisation's risk profiles has been reviewed. It also informs on tactical and strategic risk decisions with consideration of the prioritised initiatives and investments to improve the ICS key controls.
	M2.	Risk Reporting	Regular updates regarding the Group ICS Risk Profile and BRAMs must be made to the relevant Group Risk Committees and the Board. This includes the delivery of ICS Governance Committee submissions and determining the priority reports and critical risk measures required to identify, monitor, and report on the Group's material risks. Management Information (MI) and Group Risk Committees and Board submission must be established in accordance with committee timetables.
	M3.	OTCR Risk Reporting Preparation and Distribution	Preparation & distribution of the ICS Risk Appetite Metrics and other critical risk measures with explanatory commentaries to the relevant risk committees. The objective of this activity is to monitor the Group's ICS Risk exposure against appetite and where there are breaches, enable decision making to bring the exposure within appetite.
N. ICS Risk Monitoring and Reporting – Benefits Realisation	N1	Validate Risk Reduction	ICS 2LoD provides an oversight to ensure that 1LoD risk reduction activity undertaken as part of agreed ICS ERR Treatment plans results in effective risk-buydown to keep the ICS residual risk within the appetite.

Activity/Process	Sub-activity Index	Sub Activity Name	Sub Activity Description
	N2.	Group ICS Risk Profiling and Reporting	This activity is undertaken to understand what the organisation's aggregated ICS residual risk is by producing an ICS Group Aggregated Risk Profile based on the agreed aggregation methodology. This includes the provision of executive summary reports for GNFRG and reports to GRC as required (via Group Enterprise Risk Management Team).
	N3.	ICS Value Management	Value Management is the process through which value (financial and non-financial) is identified, owned, approved, maintained, measured, realised, and signed off.
O. Risk Training and Awareness	O1.	ICS Training and Awareness	To reduce the risk of a breach of Confidentiality, Integrity and Availability (CIA) of information assets due to a lack of ICS training and awareness through the delivery of training and awareness programmes to develop the desired secure behaviours that address the applicable threat scenarios and mitigate the Risk Type Framework (RTF) Risk Categories
	O2.	ICS Risk Practitioner Knowledge	The output of the process enables colleagues to up-skill, cross-skill and gain the knowledge to manage cyber risks to collectively shape a resilient bank
P. Embedding ICS Risk Culture	P1.	Define & Implement ICS Risk Culture (as applied to ICS)	To further embed a healthy risk culture as applied to ICS in the Bank and build trust and drive sustainable value for our stakeholders (including customers, partners, suppliers, and regulators), through our employees who have: (i) Constant curiosity to our threats and openness to continuous improvement (ii) Shared responsibility to defend against them (iii) Transparent and pragmatic decision making over the associated risks

Additional information on these sub-activities have been provided in the Activity One Pagers. Roles and responsibilities for each activity can be found in the ICS E2E RM&G RACI. The mentioned artefacts are available on [One Stop Shop \(sharepoint.com\)](#)

Appendix B: ICS Policies

Please refer to Part C of the ERMF

Appendix C: Version Control

Name	Key Changes	Materiality	Approved by	Version number	Approval Date
Zeeshan Arif	Initial version created as part of the consolidation of standalone RTFs during the ERMF/RTF simplification exercise.	Material	SC PLC Board	1.0	7 Dec 2023
Renzo Baio	Section 1: Clarified definition Section 5: Removed definition of Key Control Domains (KCD) as a vehicle for risk assessments. Transition from KCD to TSRA has been completed in March 2024 and they are no longer in use. Appendix C: 'Outstanding Areas of work' removed as no longer required. This section was used to highlight the areas of the ICS Framework being developed to address existing gaps.	Non-Material	Margaret Norden	1.1	29 Apr 2024
Marek Kwas/ Anita Madro	Section 1: <ul style="list-style-type: none">ICS Risk Management Principles review and alignment to overall ERMF approachOverview of ICS Risk Management Model – Figure 1 – review and update to reflect recent changes as alignment to OTCR model. Section 2: 3LoD Responsibilities review and update to reflect recent changes as alignment to OTCR model and OTCR Country Model Section 3: Decision Making Authority and Delegations review and update to reflect recent changes as alignment to OTCR model. Section 4: Regulatory Obligations and Escalation Mechanism – alignment to OR Framework and OTCR Country Model Section 5: Review and update of ICS Risk Management Components – reflecting updated ICS Risk management Governance Model Appendix A – Updated Risk management requirements incorporated into Appendix A	Material	Sadia Ricke	2.0	13 Dec 2024

Note: Please refer to Part C of the ERMF for common appendices.

----- END OF CHAPTER ELEVEN -----

----- END OF PART B -----

Part C

Appendices

C1 – Risk Taxonomy

The Risk Taxonomy can be accessed on GovPoint at the following links:

- For Non-Financial Risks click [here](#).
- For Financial Risks click [here](#).

C2 – List of Group Policies

Please refer to GovPoint for latest list.

S.No	Policy Name	Risk Framework	Document Approver
1	CIB Credit Policy	CIB Credit	Head, Policy and Process, CIB
2	Group Large Exposure Policy	CIB Credit	Head, Policy and Process, CIB
3	Secondary Distribution Policy	CIB Credit	Head, Policy and Process, CIB
4	Origination and Primary Distribution Policy	CIB Credit	Head, Policy and Process, CIB
5	Financial Markets Systematic Internaliser Policy	Compliance	Head CFCC: CIB AME, Grp Islamic, FM and TM
6	Automated Trading Policy	Compliance	Head CFCC: CIB AME, Grp Islamic, FM and TM
7	Group Relationships with Clients Policy	Compliance	Global Head, CFCC, CIB, EA, ASA and AME
8	Group Best Execution and Order Handling Policy	Compliance	Global Head, CFCC, CIB, EA, ASA and AME
9	Group Fiduciary Governance Policy	Compliance	Global Head, CFCC, CIB, EA, ASA and AME
10	Group Market Conduct Policy	Compliance	Global Head, CFCC, CIB, EA, ASA and AME
11	Group Competition and Anti-Trust Policy	Compliance	Global Head, FCC,CFCC Framework,Functions & SCV
12	Group Conflicts of Interest Policy	Compliance	Global Head, FCC,CFCC Framework,Functions & SCV
13	Group Cross Border Policy	Compliance	Global Head, FCC,CFCC Framework,Functions & SCV
14	Group Data Conduct Policy	Compliance	Global Head, FCC,CFCC Framework,Functions & SCV
15	Group Speaking Up Policy	Compliance	Global Head, FCC,CFCC Framework,Functions & SCV
16	Non-Financial Regulatory Reporting Policy	Compliance	Global Head, FCC,CFCC Framework,Functions & SCV
17	Group Individual Accountability Policy	Compliance	Global Head, FCC,CFCC Framework,Functions & SCV
18	Volcker Policy	Compliance	Global Head, Volcker and Swap Dealer Compliance
19	Digital Assets Risk Management Policy ("DA Policy")	Enterprise Level	Global Head-ERM, Dep CRO, SC Bank
20	Enterprise Stress Testing Policy	Enterprise Level	Global Head-ERM, Dep CRO, SC Bank
21	Risk Appetite Policy	Enterprise Level	Global Head-ERM, Dep CRO, SC Bank
22	Group Anti-Bribery and Corruption (ABC) Policy	Financial Crime	Global Head of FCC, Conduct & Compliance Framework
23	Group Anti-Money Laundering and Counter Terrorist Financing Policy	Financial Crime	Global Head of FCC, Conduct & Compliance Framework
24	Group Fraud Risk Management Policy	Financial Crime	Global Head of FCC, Conduct & Compliance Framework
25	Group Sanctions Policy	Financial Crime	Global Head of FCC, Conduct & Compliance Framework
26	Group Information and Cyber Security Policy	Information and Cyber Security	Global Head, OTCR, TTO
27	Group Model Risk Policy	Model	Global Head-ERM, Dep CRO, SC Bank
28	Subsidiary Governance Policy	Operational and Technology	Group Company Secretary
29	Group Contracts Policy	Operational and Technology	Global Head of Transformation, Strategy & COO
30	Group Engaging External Counsel Policy(GEEC)	Operational and Technology	Global Head of Transformation, Strategy & COO
31	Corporate Action and New Market Entry Policy	Operational and Technology	Global Head, Corporate Development
32	Group Third Party Risk Management Policy	Operational and Technology	Global Head of Operational, Technology and Cyber Risk
33	Change Governance Policy	Operational and Technology	Global Head of Operational, Technology and Cyber Risk
34	Transaction Processing Policy	Operational and Technology	Global Head of Operational, Technology and Cyber Risk

S.No	Policy Name	Risk Framework	Document Approver
35	Group Operational Risk Policy	Operational and Technology	Global Head of Operational, Technology and Cyber Risk
36	Product Governance Policy	Operational and Technology	Global Head OTCR, Framework & Stress Testing
37	Group Technology Policy	Operational and Technology	Global Head, OTCR, TTO
38	Financial Control Substantiation and Reconciliation Policy	Operational and Technology	Group Controller
39	Group Prudential Regulatory Disclosure Policy (PILLAR 3)	Operational and Technology	Group Controller
40	Financial Regulatory Reporting Policy	Operational and Technology	Group Controller
41	Management Reporting Policy	Operational and Technology	Group Head, Central Finance and Deputy CFO SC Bank
42	Financial Reporting Policy	Operational and Technology	Group Head, Central Finance and Deputy CFO SC Bank
43	Group Health, Safety and Security Policy	Operational and Technology	Group Head Property
44	Auditor Independence Policy	Operational and Technology	Audit Committee
45	Client Service Resilience Policy	Operational and Technology	Global Head OTCR, Resilience Risk
46	Group Staff Screening Policy	Operational and Technology	Chief Strategy and Talent Officer
47	Regulation of Variable Compensation Policy	Operational and Technology	Board Remuneration Committee
48	Tax Policy	Operational and Technology	Global Head, Tax
49	Reputational Risk Policy	ESG and Reputational	Global Head-ERM, Dep CRO, SC Bank
50	Environmental, Social and Governance Risk Policy	ESG and Reputational	Global Head-ERM, Dep CRO, SC Bank
51	Traded Risk Policy	Traded	Global Head, Traded Risk Management
52	Capital Management Policy	Treasury	Global Head-ERM, Dep CRO, SC Bank
53	Interest Rate Risk In The Banking Book (IRRBB) Policy	Treasury	Global Head-ERM, Dep CRO, SC Bank
54	Liquidity and Funding Risk Policy	Treasury	Global Head-ERM, Dep CRO, SC Bank
55	WRB Credit Risk Management Policy	WRB Credit	CRO, WRB

C3 - List of Priority Reports

RTF Chapter	Risk Report	High level content / Purpose	Produced by	Frequency	Reported to
Compliance	Compliance Risk Information Report (Compliance Risk component submission to GRIR and BRIR)	Provides senior executives with an update on the compliance risk profile within the Group.	Compliance risk reporting team	Monthly	GRC / BRC
Treasury	Capital +	Actual and forward looking view of the Group's capital ratios against the regulatory limits and risk appetite.	Treasury Capital	Monthly	PRA, BoE
Treasury	MREL+	Actual and forward looking view of equity, capital and MREL eligible debt liability.	Treasury Capital	Quarterly	PRA, BoE
Treasury	OBSF	Actual and forward looking view of Group and Solo's capital ratios against the regulatory limits and risk tolerances.	Treasury Capital	Each Committee	OBSF
Treasury	GALCO	Actual and forward looking view of Group and Solo's capital ratios against the regulatory limits and risk tolerances.	Treasury Capital	Each Committee	GALCO
Treasury	GRIR	Actual and forward looking view of Group and Solo's capital ratios against the regulatory limits and risk tolerances.	Treasury Capital	Each Committee	GRC
Treasury	Structural FX	Impact to the Group's CET1 ratio on the basis of a 20 percent depreciation in material currencies against the USD.	Treasury Capital	Monthly	GALCO, GRC
Treasury	SC ALCO	Actual and forward looking view Solo capital ratios against the regulatory limits and risk tolerances	Treasury Capital	Each Committee	ALCO
Treasury	CFG (Capital Forecasting Group)	Actual and forward looking view of Group and Solo's capital ratios against the regulatory limits and risk tolerances.	Treasury Capital	Forthightly	Senior Management
Treasury	LCR – Group (DA) LCR – Solo (DA)	LCR is reported to the PRA and inputs into the GALCO report (and other internal management reports) used for effective risk management of Liquidity and Funding Risk.	GFS Liquidity Regulatory Reporting	Weekly and monthly	PRA (weekly) and GALCO
Treasury	LCR Low point (Group) – PRA110 Group LCR Low point (Solo) – PRA110 Solo	CFMR is reported to the PRA on a weekly basis.	GFS Liquidity Regulatory Reporting	Weekly	PRA
Treasury	NSFR – Group (CRR) NSFR – Solo (CRR)	NSFR is reported to the PRA and inputs into the GALCO report (and other internal management reports) used for effective risk management of Liquidity and Funding Risk.	GFS Liquidity Regulatory Reporting	Monthly (top 4 countries only) and quarterly	PRA (quarterly) and GALCO
Treasury	ADR tracker	Advances to Deposits Ratio (ADR) – Group inputs into the GALCO report (and other internal management reports) used for effective risk management of Liquidity and Funding Risk.	Performance Analytics & Planning	Monthly	OBSF, GALCO, GRC and BRC

RTF Chapter	Risk Report	High level content / Purpose	Produced by	Frequency	Reported to
Treasury	Global Weekly Liquidity Risk Report (GWLRR)	Wholesale Borrowing External ('WBE') -Group/Solo inputs into the GALCO report (and other internal management reports) used for effective risk management of Liquidity and Funding Risk.	GFS Treasury Risk	Weekly	OBSF, GALCO, GRC and BRC
Treasury	Survival Horizon Report (Group & Country)	Survival Horizon inputs into the GALCO report (and other internal management reports) used for effective risk management of Liquidity and Funding Risk. The report includes Solo USD SH	GFS Treasury Risk	Daily and Monthly	Monthly to OBSF, GALCO, GRC and BRC
Treasury	Market Wide Stress (MWS) Report (country specific)	Any breach to 60 days MWS is reported on a monthly basis to various Group level committees used for effective risk management of Liquidity and Funding Risk.	GFS – Treasury Risk	Monthly	OBSF, GALCO, GRC and BRC
Treasury	Net Interest Income ("NII")	Report 1: Parallel Shift up (Regulatory scenario; monthly monitoring and pillar 3 disclosure every 6 months.)	GFS Treasury IRRBB	Monthly	Monthly reporting to Group level committees including, OBSF, GALCO, GRC and BRC.
		Report 2: Parallel Shift down: (Regulatory scenario; monthly monitoring and pillar 3 disclosure every 6 months.)			
		Report 3: NII sensitivity risk appetite (Board RA scenario, limits are set against this)			
		Report 4: +50 bps (Internal scenario; monthly monitoring in ALCO and disclosed as part of financial statements every 6 months)			
		Report 5: -50 bps (Internal scenario; monthly monitoring in ALCO and disclosed as part of financial statements every 6 months)			
		Report 6: 100 bps (Internal scenario; monthly monitoring in ALCO and disclosed as part of financial statements every 6 months)			
Treasury	Economic Value of Equity ("EVE")	Report 1: Parallel Shift up (Board RA, limits are set against this - Regulatory scenario; monthly monitoring and pillar 3 disclosure every 6 months)	GFS Treasury IRRBB	Monthly	Monthly reporting to Group level committees including, OBSF, GALCO, GRC and BRC.
		Report 2: Parallel Shift down (Regulatory scenario; monthly monitoring and pillar 3 disclosure every 6 months)			
		Report 3: Short rates up (Regulatory scenario; monthly monitoring and pillar 3 disclosure every 6 months)			
		Report 4: Short rates down (Regulatory scenario; monthly monitoring and pillar 3 disclosure every 6 months)			
		Report 5: Flatteners (Regulatory scenario; monthly monitoring and pillar 3 disclosure every 6 months)			
		Report 6: Steepener (Regulatory scenario; monthly monitoring and pillar 3 disclosure every 6 months)			
		Report 7: ICAAP (Annual ICAAP submission)			
Treasury	Non-Traded Market Risk – T22	Report 3: Stress Test Data Framework – T22: (Repricing gap profile of the balance Sheet with balances to being tied back to IFRS/FINREP)	GFS Treasury IRRBB	Quarterly	PRA

RTF Chapter	Risk Report	High level content / Purpose	Produced by	Frequency	Reported to
Treasury	Pension Risk Information Report	Monitoring pension risk against pre-defined appetite levels and escalation triggers	Group Pensions	Monthly, except following quarter ends	Global Head ERM Head Scenario Design, Country Risk
Treasury	Pension Risk ICAAP & BOE stress testing report	Summarise the Pension Risk results for input into the Group's stress tests for ICAAP and Bank of England	Group Pensions	Twice annually	EST
Traded	BRIR (BRC)	Management Information pack covering Stress Testing, WWR	TRR	Every 2 months	TRM / FO
Traded	GRIR (GRC)	Management Information pack covering Stress Testing, WWR	TRR	Monthly	TRM / FO
Traded	CIBRIR (CIBRC)	Management Information pack covering Stress Testing, WWR, Key Limits and Capital	TRR		
Traded	Traded Risk Stress Summary	To monitor material risks and effective risk management to set risk appetite in line with strategic objectives	TRR	Weekly	TRM / FO / Group Risk
Traded	Traded Risk Appetite Report	To monitor material risks and effective risk management to set risk appetite in line with strategic objectives	TRR	Weekly	TRM/ Group Risk
Traded	Backtesting Confirmation	To monitor material risks and limits in line with strategic objectives	TRR	Daily	TRM / MRA / PC
Traded	Group VaR	To monitor material risks, monitor limits and/or provide Risk Appetite metrics	TRR	Daily	TRM / FO
Traded	Market Risk Capital/RWA Report	Report of Group and Solo market risk regulatory capital requirements-RWA.	Market Risk Capital Management	Monthly	Mkt Risk Capital-Monthly Capital Report (Email group)
Traded	FM Credit Exposure Report	Report is used to monitor material risks, monitor limits and/or provide Risk Appetite metrics	TRR	Daily	TRM / FO
Traded	FM Secured Financing	Report is used to monitor material risks, monitor limits and/or provide Risk Appetite metrics	TRR	Fortnightly	TRM / FO
Credit WRB	WRB Risk Committee Pack	Which also covers: GRIR (Group Risk Information Report) : WRB section; RAMI reports (Risk Appetite Metrics; Group RDF MI reports; AFPQR as a dataset to prepare the report	Group Risk Reporting, WRB team	Monthly	GRC, BRC
Credit WRB	Stress Testing Data Framework (and templates 13 and 14)	Portfolio Quality information by "Mortgage" and "Excluding Mortgage" Prudential Regulation Authority ("PRA") defined templates and definitions. This information is used for submissions to the PRA (as well as year "0" information for the yearly BoE stress testing exercises.	Country and Group Risk Reporting, WRB team	Quarterly	PRA
Credit WRB	Portfolio Quality pack	Acquisition, Portfolio Quality and Collections information sourced from all countries to form a repository for multiple reports. This is currently produced centrally for 14 countries and is used for Portfolio reviews. (Incorporates AFPQR)	Country and Group Risk Reporting, WRB team	Monthly	Group and Country WRB Credit Risk
Credit CIB	Past Due and Forbearance Report	The purpose of this report is to prepare and submit Past due & Forbearance Report to the finance team. For this report we gather past due and forbearance numbers from individual countries and SAR.	Credit Risk Reporting & MI	Quarterly	Mailbox:FinrepReport, FR (final recipient is PRA)

RTF Chapter	Risk Report	High level content / Purpose	Produced by	Frequency	Reported to
Credit CIB	Group Risk Information Report (GRIR- Credit Risk Reporting & MI)	The purpose for this report is to provide Group-level analysis of risks listed in the Risk Management Framework. Risk such as Information & Cyber Security, Compliance, FCC, Conduct, Reputational are under review to be included as separate sections	Credit Risk Reporting & MI	Monthly	Group Risk Committee (GRC)
Credit CIB	Stress Testing Data Framework (STDF)	Stress Test Data Framework (STDF) Actuals from Credit Risk (Corporate & Institutional Commercial and PvB), is submitted to the PRA on a Quarterly/Annual basis. Separate Actuals templates are also submitted to the Portfolio Risk team and the data from these forms the actuals data which show the position of the firm at the start of the stress.	Credit Risk Reporting & MI	Quarterly/Annual	Bank of England
Credit CIB	Crisis Reports	To report the key risk metrics for the crisis reporting under identified scenarios of Crisis, in order to help the Senior Risk Managers, evaluate necessary remediation actions and decisions	Credit Risk Reporting & MI	Ad-hoc	Senior Officer in Credit Risk Management (SCO and above) or Early Alert Committee.
Credit CIB	Risk Review with Rating Agencies	These are the sessions where the rating agencies meet senior management and are a key component of the rating agencies' review process and are instrumental in the rating committee discussions. The annual review sessions is to address the rating agencies concerns and ensure they have the right understanding of the new strategy and disclosures made.	Credit Risk Reporting & MI (across PRTs) – Produced by respective PRTs and collated by Credit Risk Reporting & MI.	Semi- annually/ Annually	Group Treasury team
ICS	PLC Board Report	Information relating to board risk appetite metric positions and breaches, and the Group ICS risk profile	Group CISRO	As required	Group ERM
ICS	Board Risk Committee Risk Information Report	Information relating to board risk appetite metric positions and breaches, and the Group ICS risk profile	Group CISRO	As required	Group ERM
ICS	Group Risk Information Report	Information relating to board risk appetite metric positions and breaches, and the Group ICS risk profile	Group CISRO	As required	Group ERM
ICS	Group Non-Financial Risk Committee Report	Information relating to board risk appetite metric positions and breaches	Group CISRO	As required	GNFRC
O & T	Common Reporting Requirements (COREP)	Provide Operational Loss information in accordance with Regulatory requirements	Operational Risk (OR) Reporting (GBS India)	Half-yearly	European Banking Authority
O & T	Stress Test Data Framework (STDF)	Provide Operational Loss information in accordance with Regulatory requirements	OR Reporting (GBS India)	Annually	Prudential Regulation Authority
O & T	FSA072 & 073	Provide Operational Loss information in accordance with Regulatory requirements	OR Reporting (GBS India)	Annually	Bank of England
O & T	Group Non-Financial Risk Committee Risk Information Report (GNFRC)	Provide the Group Non-Financial Risk Committee with relevant Operational Risk Management information	OR Reporting (GBS India) OR Reporting (Singapore)	Monthly	GNFRC

RTF Chapter	Risk Report	High level content / Purpose	Produced by	Frequency	Reported to
O & T	Group Risk Information Report (GRIR) (component submission by OR)	Provide the Group Risk Committee with relevant Operational Risk Management information	OR Reporting (GBS India) OR Reporting (Singapore)	Monthly	GRC
O & T	Board Risk Information Report (BRIR) (component submission by OR)	Provide the Board Risk Committee with relevant Operational Risk Management information	OR Reporting (GBS India) OR Reporting (Singapore)	Once every 2 months	BRC
O & T	Group Enterprise Stress Testing (Group EST)	Specify the extraction criteria and controls associated with production of Group Operational Risk Stress Test Data Report (GOR-STDR) for use in Group Internal Capital Adequacy Assessment Process (ICAAP) and Enterprise Stress Testing (EST) process	OR Reporting (GBS India)	Quarterly	Bank of England
Model	Group Model Risk Update Report	The Group Model Risk Update Report ("GMRU") provides detail on Risk Appetite ("RA") metrics for Model Risk. It supports internal risk management and contributes to the Group and Board Risk Information Reports ("GRIR/BRIR") that are submitted to Group Risk Committee ("GRC") and Board Risk Committee ("BRC"). The GMRU provides senior management with an update on the Bank's model risk management, with a focus on high-risk models, unfavourable model validation outcomes, material model issues, the model landscape and model risk appetite.	Model Risk Policy and Governance	Monthly, in line with GRC and BRC committee schedule	GRC and BRC
Model	Quarterly Model Risk Management Metric Report	The Quarterly Model Risk Management Metric Report ("QMMR") is used for internal risk management within model risk and is shared with the Model Risk Committee ("MRC"). The report provides senior management with an overview of the Bank's model risk profile through management metrics and details on the model landscape. The report covers model risk statistics for all elements of the Model Life-Cycle ("MLC") which allows identification, monitoring and reporting of key model risks to senior management on a periodic basis.	Model Risk Policy and Governance	Quarterly, in line with MRC committee schedule	MRC
ESG & Reputational Risk	Reputational and Sustainability Risk ("RSR") Group Risk Information Report ("GRIR")	The RSR GRIR includes risk information and risk appetite metrics (including details on risk metrics and breaches, if any).	Risk & CFCC Reporting	Monthly	GRC/BRC

RTF Chapter	Risk Report	High level content / Purpose	Produced by	Frequency	Reported to
ESG & Reputational Risk	Group Risk Information Report ("GRIR") Board Risk Information Report ("BRIR") Climate Risk Management Committee Risk Report	Reporting and risk appetite metrics across: - Credit Risk (CIB and WRB) - Operational and Technology Risk - Country Risk - Traded Risk	Group Risk Reporting	Quarterly	CRMC, GRC, BRC

C4 – Group Risk Assessment Matrix & Country Risk Assessment Matrix

GROUP RISK ASSESSMENT MATRIX						
Likelihood	Likelihood definitions	Label				
Very High	Very High likelihood of occurrence (over next 12 months)	E	LOW	MEDIUM	MEDIUM	HIGH
High	High likelihood of occurrence (over next 12 months)	D	LOW	LOW	MEDIUM	VERY HIGH
Medium	Medium likelihood of occurrence (over next 12 months)	C	LOW	LOW	MEDIUM	VERY HIGH
Low	Low likelihood of occurrence (over next 12 months)	B	LOW	LOW	MEDIUM	HIGH
Very Low	Very Low likelihood of occurrence (over next 12 months)	A	LOW	LOW	LOW	HIGH

FINANCIAL IMPACT (Group)	1	2	3	4	5
Financial Loss (USD)	Operational Loss of less than USD 20 Mio	Operational Loss of >=USD 20 Mio and <USD 50 Mio	Operational Loss of >=USD 50 Mio and <USD 100 Mio	Operational Loss of >=USD 100 Mio and < USD 200 Mio	Operational Loss of >=USD 200 Mio

COUNTRY RISK ASSESSMENT MATRIX						
Likelihood	Likelihood definitions	Label				
Very High	Very High likelihood of occurrence (over next 12 months)	E	LOW^c	HIGH^c	HIGH^c	VERY HIGH
High	High likelihood of occurrence (over next 12 months)	D	LOW^c	MEDIUM^c	HIGH^c	VERY HIGH
Medium	Medium likelihood of occurrence (over next 12 months)	C	LOW^c	MEDIUM^c	HIGH^c	VERY HIGH
Low	Low likelihood of occurrence (over next 12 months)	B	LOW^c	MEDIUM^c	HIGH^c	HIGH
Very Low	Very Low likelihood of occurrence (over next 12 months)	A	LOW^c	LOW^c	MEDIUM^c	HIGH

FINANCIAL IMPACT (Country)	1	2	3	4	5
Financial Loss (USD)	Tier 1: <\$0.5m Tier 2: <\$ 0.1m	Tier 1: >\$0.5m <\$50m Tier 2: >\$0.1m <\$50m	≥ \$50m < \$100m	≥ \$100m < \$200m	≥ \$200m

NON-FINANCIAL IMPACT (Group & Country)					
REGULATORY	Administrative penalties leading to no further regulatory action	Formal private regulatory warnings or censures or minor financial penalties. Or Material negative feedback within a formal regulatory inspection report where no formal regulatory rating exists	Public censure by a regulator Or Material suspension or delays in the granting of approvals for new business or new licenses Or Criminal or civil investigations or proceedings against the country or its management team or directors Or Adverse impact to the formal regulatory rating where one exists	Material enforcement measures requiring ongoing monitoring of a country's business activities and the requirement to report to such monitor on a regular basis over a period of at least 12 months	Very material suspension of business or license approvals Or Suspension of entire country banking license Or Adverse capital guidance from a prudential regulator Or Material criminal or civil investigations or proceedings against the group or its directors
CUSTOMER (INCLUDING REPUTATIONAL)	Media Minimal adverse media coverage in local or international media.	Media Short-term (<=3 months) adverse media coverage in local or international media.	Media Sustained (>3 months) adverse media coverage in local or international media.	Media Sustained (>3 months) adverse media coverage in local or international media with temporary damage to the brand (less than 1 year)	Media Sustained (>3 months) adverse coverage in local or international media with lasting damage to the brand (more than 1 year).
	Clients and critical stakeholders Minimal impact to clients and / or investors This could also be due to NGO activism.	Clients and critical stakeholders Immaterial isolated cases impacting clients and / or investors in an adverse manner This could also be due to NGO questions over business practices.	Clients and critical stakeholders Material adverse impact to a large number of clients and / or investors through a systemic breakdown; This could also be due to NGO questions over specific perceived lapses in standards or business choices	Clients and critical stakeholders Very material adverse impact to an entire segment of the client population and / or a large number investors This could also be due to public disclosures by NGOs over specific perceived lapses in standards or business choices; using social media to campaign against the Group	Clients and critical stakeholders Significant adverse impact to all clients in multiple client segments and / or all investors This could also be due to disruptive actions by NGOs impacting business continuity
	Consequential reputational risk from ICS events ^{**} No impact to clients and/or staff or continuity of business due to either of / a combination of any of the following: 1. Temporary or permanent loss of Information Confidentiality 2. Temporary or permanent loss of Information Availability 3. Temporary or permanent loss of Information Integrity	Consequential reputational risk from ICS events ^{**} Low impact to clients and/or staff or continuity of business due to either of / a combination of any of the following: 1. Temporary or permanent loss of Information Confidentiality 2. Temporary or permanent loss of Information Availability 3. Temporary or permanent loss of Information Integrity	Consequential reputational risk from ICS events ^{**} Material adverse impact to clients and/or staff or continuity of business due to either of / or a combination of any of the following: 1. Temporary or permanent loss of Information Confidentiality 2. Temporary or permanent loss of Information Availability 3. Temporary or permanent loss of Information Integrity	Consequential reputational risk from ICS events ^{**} Very material adverse impact to an entire segment of the client population and/or large number of staff, or continuity of business due to either of / a combination of any of the following: 1. Permanent loss of Information Confidentiality 2. Permanent loss of Information Availability 3. Permanent loss of Information Integrity	Consequential reputational risk from ICS events ^{**} Severe adverse impact to multiple segments of the client population and/or all staff, or continuity of business due to either of / a combination of any of the following: 1. Permanent loss of Information Confidentiality 2. Permanent loss of Information Availability 3. Permanent loss of Information Integrity
SAFETY & SECURITY	No treatment or first aid only	Minor medical treatment (clinic, doctor, ER). Medical leave. Hospitalisation for up to 48 hours	Serious injuries. Hospitalisation as inpatient (+48 hours) or permanent partial disability	Single fatality, permanent total disability or multiple major injuries.	Multiple fatalities or permanent total disabilities

^{**} Consider all the items listed under sub-outcome "Consequential reputational risk from ICS events" for rating technology events (in addition to all other outcomes)

Tier 1 Countries: Hong Kong, Singapore, South Korea, India, China, UK, UAE, United States of America

Tier 2 Countries: All other countries

HIGH^c	Country High
MEDIUM^c	Country Medium
LOW^c	Country Low

C5 - List of Group Standards to Frameworks

S.No	Standard Name	Risk Framework	Document Approver
1	Group Electronic and Voice Communications Standard	Compliance	Global Head of Frameworks and Policies
2	Group Communications with Regulators Standard	Compliance	Global Head, Regulatory Engagement & Advocacy
3	Standard for Managing Regulatory Change by Compliance, Financial Crime and Conduct Risk (CFCR)	Compliance	Global Head of Frameworks and Policies
4	Risk Data Aggregation Standard (RDAS)	Enterprise Level	TTO-CIO-Functions
5	Risk Reporting Standards	Enterprise Level	COO Risk & CFCC
6	Group Conduct Risk Management Standard	Enterprise Level	Global Head of Frameworks and Policies
7	Framework and Policy Governance Standards (FPGS)	Enterprise Level	Global Head-ERM, Dep CRO, SC Bank
8	Entity Risk Governance Standard (ERGS)	Enterprise Level	Global Head-ERM, Dep CRO, SC Bank
9	Group Investigations Standard	Enterprise Level	Global Head-ERM, Dep CRO, SC Bank
10	Country Risk Standards	Enterprise Level	Global Head-ERM, Dep CRO, SC Bank
11	Committee Governance Standards	Enterprise Level	Global Head-ERM, Dep CRO, SC Bank
12	Risk Assessment of New Initiatives	Enterprise Level	Global Head-ERM, Dep CRO, SC Bank
13	Effectiveness Review Standard	Enterprise Level	Global Head-ERM, Dep CRO, SC Bank
14	Risk, Cause and Control Taxonomies Standard	Enterprise Level	Global Head-ERM, Dep CRO, SC Bank
15	Interim Risk Governance Standard	Enterprise Level	Global Head-ERM, Dep CRO, SC Bank
16	Group Standard for Tackling Domestic Violence and Abuse	Operational and Technology	Chief Strategy and Talent Officer
17	Group Flexi-Worker Standard	Operational and Technology	Chief Strategy and Talent Officer
18	Group Grievance Standard	Operational and Technology	Chief Strategy and Talent Officer
19	Group Redundancy Standard	Operational and Technology	Chief Strategy and Talent Officer
20	Group Disciplinary Standard	Operational and Technology	Chief Strategy and Talent Officer
21	Group Pensions and Benefits Standard	Operational and Technology	Chief Strategy and Talent Officer
22	Group Related Party Transaction Standard	Operational and Technology	Group Company Secretary
23	Group International Mobility (IM) Standard	Operational and Technology	Chief Strategy and Talent Officer
24	Group Business Expenditure Standard	Operational and Technology	Global Head, SCM Transformation
25	Group Diversity and Inclusion Standard	Operational and Technology	Chief Strategy and Talent Officer
26	People Leader Standard	Operational and Technology	Chief Strategy and Talent Officer
27	Changes to Group Corporate Structure Standard	Operational and Technology	Group Company Secretary
28	Group Employee Referral Standard	Operational and Technology	Chief Strategy and Talent Officer
29	Group Student Hiring Standard	Operational and Technology	Chief Strategy and Talent Officer
30	Contractual Recognition Of Bail-In (Article 55) Standards	Treasury	Head, Treasury Recovery and Resolution Planning
31	Pension Risk Standard	Treasury	Head, Pensions & Reward Analytics
32	Resolution Standard	Treasury	Head, Treasury Recovery and Resolution Planning
33	Group Recovery Plan Standard	Treasury	Head, Treasury Recovery and Resolution Planning
34	Intragroup Accounts Standard	Treasury	Regional TCRO, ASA & AME
35	Debt Issuance Standard	Treasury	MD, Head, Capital Issuance & Term Funding
36	Banking Book Funds Transfer Pricing (FTP) Standard	Treasury	Managing Director, Global Head, Treasury Liquidity
37	Financial Markets Funds Transfer Pricing Standard	Treasury	Managing Director, Global Head, Treasury Liquidity

C6 – List of Group Processes & Controls

Central list can be accessed on SharePoint by clicking [here](#).

C7 – Change Log

Name	Key Changes Made	Materiality	Approved by	Version No.	Date
Aparna Rajgopal	<ul style="list-style-type: none"> Revised PRT definitions to align with the Risk Type Frameworks approved in Jul'18 (Section 5, Table 2) Clarified delegations of authority to implement this framework and manage Principal Risks (Section 7.3). Clarified approach to policies to make it principle based with actionable statements to control and mitigate critical risks (Section 6.3). Updated Group Risk Appetite review process (Section 9) and added the approach to cascading of the Group Risk Appetite metrics to countries with significant business operations (Section 14) 	Non-material	Mark Smith	1.1	7 Nov 2018
Aparna Rajgopal	<ul style="list-style-type: none"> ERMF to be read in conjunction with SCB Responsibilities Map (Section 1.4) Second Line of Defence responsibility in curtailing business extended to cover material policy non-compliance or when operational controls are ineffective in managing risks (Section 4, Table 1) Revised definition of Traded Risk (Section 5, Table 2) Expanded the Executive and Board-level committee coverage to include Brand, Value and Conduct Committee 	Non-material	Mark Smith	1.1	22 Feb 2019
Aparna Rajgopal	<ul style="list-style-type: none"> Elevated Model Risk to a Principal Risk Type (Section 5). In addition to Principal Risk Types, the Group recognises material cross-cutting risks such as Climate Risk that materialise through other Principal Risk Types (Section 5) Incorporated Group Risk Appetite Statements. Introduced forward-looking or stress scenario considerations in setting Group Risk Appetite thresholds, where applicable. Level 3 Risk Appetite metrics removed as these are assigned to management-level monitoring. Recovery indicators integrated into the ERMF (Section 9) Updated to reflect Group Risk Committee and Group Asset and Liability Committee derive their authorities from the Group Chief Risk Officer and Group Chief Financial Officer respectively. Removed references to Court (Section 8) Clarified regulatory attestation requirements (Section 13) Formalised the annual self-assessment process for branches/ subsidiaries to assess the overall adoption and effectiveness of ERMF locally (Section 14) 	Material	SC PLC Board	2.0	12 Dec 2019
Aparna Rajgopal	<ul style="list-style-type: none"> Amended the definition of Financial Crime to include Fraud (Section 5, Table 2) 	Non-material	Mark Smith	2.1	9 Jan 2020
Aparna Rajgopal	<ul style="list-style-type: none"> Updated the definition of Information and Cyber Security to align with the 2020 RTF (Section 5) Replaced Control Assessment Standards (CAS) with Risk and Control Self-Assessment (RCSA) in-line with the new Operational Risk Type Framework, Policy and Standard Included the Board approved Risk Appetite Statement for Model Risk (Section 8) With the retirement of the Validation and Effectiveness Review Standard (VERS), references updated to Framework and Policy Governance Standards (for effectiveness reviews and regulatory attestations) and Operational Risk Policy and Standard (for validation of internal controls) (Section 13) 	Non-material	Mark Smith	2.2	14 Jul 2020

Name	Key Changes Made	Materiality	Approved by	Version No.	Date
	<ul style="list-style-type: none"> Risk management for branches, subsidiaries and non-banking subsidiaries updated to align with the Enterprise Risk Governance Standard (Section 14) 				
Veesha Jotangia	<ul style="list-style-type: none"> Expanded the Reputational Risk Principal Risk Type to “Reputational and Sustainability” to integrate ESG risk management with a focus on “Do No Significant Harm” and “Responsible Business Conduct” across clients, third party and own operations (Section 6). Country Risk management elevated as an integral component of the ERMF within the section on Group strategy and strategic risk management (Section 3). This approach will replace Country Risk as a principal risk type. Conduct Risk Management elevated as an integral component of the ERMF (Section 4). This approach will replace Conduct as a principal risk type. Expanded the Operational Risk Principal Risk Type to “Operational and Technology” (Section 6) Clarified that Global Head, ERM has second line responsibilities for Climate Risk and will set a Climate Risk Standard (Section 6). Following the transfer of Stress Testing from Risk to Finance, clarified that that Group Chief Financial Officer delegates first line responsibility for Stress Testing to the Group Head, Finance. The GCRO retains second line responsibility and delegates to the Global Head, ERM (Section 11) The Risk Data Aggregation Standards, which sets the minimum standards for driving strategy to enhance risk data aggregation capabilities is mapped to the ERMF (Section 13) 	Material	SC PLC Board	3.0	10 Dec 2020
Veesha Jotangia	<ul style="list-style-type: none"> Group Risk Appetite Statements table updated to align to interim changes approved by the Board Risk Committee in May 2021 (section 10, Table 3) 	Non-material	Mark Smith	3.1	1 Jul 2021
Veesha Jotangia	<ul style="list-style-type: none"> Amended to reflect that Board level oversight for Conduct Risk Management now sits with the Audit Committee (Section 4) Role of OR in providing oversight adjusted wording to clarify that this is in the context of RCSA and Response Management (Section 5 & Section 8) Capital & Liquidity renamed to “Treasury”, definition expanded to include IRRBB and RFO responsibility transferred from Group Treasurer to Group Head, ERM (Section 6) (Section 11) Renaming of “material cross-cutting risk” to “Integrated risk type” (Section 7) Introduction of a new Integrated Risk section which sets out the definition of Integrated risk types, roles and responsibilities for Integrated Risk Framework Owners and RFOs, and minimum governance requirements (Section 7) Inclusion of Digital Asset Risk and Third-Party Risk as integrated risk types (Section 7) Risk Appetite updated to reflect split between Group Board level RA and Group Management Team level RA (Section 11) Enhancement of RCSA statement to clearly set out the minimum steps and requirements (Section 13) Differentiation between a “Risk Taxonomy” which includes PRTs, IRTs and risk sub types inherent to the strategy and business model, and an “Emerging Risks Inventory” (Section 13) Responsibility for Risk Data Aggregation Standards and Risk Reporting Standards sits with CIO Functions and COO Risk & CFCC respectively (Section 14) 	Material	SC PLC Board	4.0	15 Feb 2022
Veesha Jotangia	<ul style="list-style-type: none"> Inclusion of responsibilities related to IBS (Section 5) Simplification of the definition for Treasury Risk (Section 6) Transfer in second line oversight of Third Party Risk from Global Head, Supply Change Management to Global Head of Risk, Functions and Operational Risk (Section 7) 	Non-material	Mark Smith	4.1	30 Jun 2022

Name	Key Changes Made	Materiality	Approved by	Version No.	Date
	<ul style="list-style-type: none"> Change in review frequency of RTFs from annual to once every 2 years (Section 8) Updated RA statements for Treasury and Traded (Section 11) Change in appointment authority for Subsidiary ERC (Section 16) 				
Zeeshan Arif	<ul style="list-style-type: none"> Sec 4.1, 4.3: Scope expanded to include 'impact to environment' as additional consideration when making strategic decisions. Sec 10 – updated Committee Structure by removing BFCRC. Sec 11.5: Risk Appetite – Inclusion of Risk Appetite allocation mechanism and calibration principles. Sec 15.2: Effectiveness Review and Regulatory Attestation moved to a newly introduced standard 'ERS' Sec 15.9: SC Ventures is out of scope of the requirements defined by this framework. Removed Board Financial Crime Risk Committee and any reference to it. Sec 16.2 local variations to ERMF and RA can go directly to local governance committee without ERM review. Sec 16.5 – Effectiveness Review frequency change to two years for branches. Sec 17 – Updated Glossary 	Material	SC PLC Board	5.0	08 Dec 2022
Zeeshan Arif	<ul style="list-style-type: none"> Scope - Clarified scope of the ERMF with regards to SC Ventures. Updated Risk Culture definition. Group Strategy and Strategic Risk Management - Clarified processes for corporate planning strategic review and risk identification. Updated roles and responsibilities. Conduct Risk - Updated text with reference to the new Conduct Standard. Three LoD - Updated 1LoD and 2LoD sections to align with redefined Process Owner and Policy Owner responsibilities. Aligned to the third line of defence (Group Internal Audit) section to Audit Charter. PRTs - Section expanded to include approach and coverage of other areas of risk governed by policies directly linked to the ERMF (e.g., Digital Assets, Climate, Third Party). Integrated Risk - Discontinued the use of IRT concept and IRT Owners role. Control Framework, Roles and Responsibilities - Updated in line with RTFs repositioning within ERMF; clarified Policy Owner responsibilities and any handoff to Process Owner (see Appendix A). Source of Authorities - Minor update in line with RTFs repositioning into ERMF. Group RA Statement - Clarified when the Group is considered to be within RA. Enterprise Stress Test - Minor update in line with RTFs repositioning into ERMF. Enterprise Risk ID, Assessment, Mitigation and Monitoring - High level refresh; removed reference to Risk and Control Self-Assessment as the sole basis for risk identification for the Group. Risk Data Aggregation, Risk Reporting and Data Quality - Updated in line with RTFs repositioning and aligned with latest policies and standards. Validation, Effectiveness Review and Independent Assurance - Updated in line with RTFs repositioning and revised Policy Owner responsibilities. Risk Management for Branches and Subsidiaries - Updated in line with RTFs repositioning including coverage of local regulatory obligations. 	Material	SC PLC Board	6.0	07 Dec 2023

Name	Key Changes Made	Materiality	Approved by	Version No.	Date
	<p>New Sections</p> <ul style="list-style-type: none"> Policy Owner and Process Owner Responsibilities (Replacing part of Section.8) - The 2LoD Policy Owner and 1LoD Process Owner responsibilities have been revised to provide a complete and comprehensive understanding of their responsibilities and with the aim to facilitate adherence to regulatory obligations. General Principles and Governance of RTFs (New Part B, Section.1) Introductory section to include common/generic text and requirements across the RTFs now repositioned into the ERMF. RTFs - (New sections in ERMF – Part B Streamlined RTFs and repositioning within ERMF (Part B). 				
Ioana Cornisteanu	<ul style="list-style-type: none"> Conduct Risk Management: Included delegation from Group Head, CFCC to Global Head of Frameworks and Policies for responsibility for Conduct Risk Management. Three LoD: Clarified oversight and challenge requirements in situations where a Function acts as both First Line of Defence (1LoD) and Second Line of Defence (2LoD) Committees and Meetings: Added definition of “committee”, distinguishing it from other types of governance meetings. Control Framework, Roles and Responsibilities: Removal of Risk Sub-Types (Risk Frameworks now align to the new Risk Taxonomy). Clarified provisions 8.5.3(I)(c) and 8.5.3 (II). RA Framework: Included delegations of authority from the Board to allow for changes in Risk Appetite thresholds outside of the interim and annual review cycles. Included approval authorities for Out of Cycle MTL changes. EST: Included Climate Risk Stress Test for assessment of physical and transition risks associated with climate related scenarios. Risk Reporting, Risk Data Aggregation and Data Quality: Updated to align to Basel Committee of Supervision 239 regulations and to enhance clarity of internal requirements. Country Risk: Repositioned to a dedicated section for enhanced clarity and focus, maintaining the linkage to ERMF while allowing for more detailed discussion and accessibility to Country Risk related information 	Material	SC PLC Board	7.0	26 Jul 2024
Ioana Cornisteanu	<ul style="list-style-type: none"> Clarified oversight responsibilities over 2LoD functions performing their own operational activities (Section 4.3) Included cross reference to ERMF common appendices for the list of delegates for approval of policies and standards (Section 5.5) Updated PRT name, definition, and RA statement for ESGR. 	Non-Material	Sadia Ricke	7.1	19 Dec 2024

C8 – List of Group Abbreviations, Acronyms and Terms

For updated listed of acronyms and terms, please use the link below.

[Governance Libraries - ERM Glossary of Terms - All Items \(sharepoint.com\)](#)

Term	Definition
AC	Audit Committee
BoE	Bank of England
Board	Standard Chartered PLC Board of Directors
BRC	Board Risk Committee
CCRO	Country Chief Risk Officer
CEO	Chief Executive Officer
CFCC	Conduct, Financial Crime and Compliance
CFO	Chief Financial Officer
CRO	Chief Risk Officer
CRC	Country Risk Committee
CSC	Culture and Sustainability Committee
DOI	Department Operating Instructions
ERC	Executive Risk Committee
ERGS	Entity Risk Governance Standard
ERS	Effectiveness Review Standard
ERM	Enterprise Risk Management
ERMF	Enterprise Risk Management Framework
FPGS	Framework and Policy Governance Standard
GALCO	Group Asset and Liability Committee
GCEO	Group Chief Executive Officer
GCFO	Group Chief Financial Officer
GCRO	Group Chief Risk Officer
Global Head, ERM	Global Head, Enterprise Risk Management
Group	Branches and Banking Subsidiaries of Standard Chartered PLC
Group Head, CFCC	Group Head, Conduct, Financial Crime and Compliance
GRC	Group Risk Committee
ICAAP	Internal Capital Adequacy Assessment Process
LoD	Line of Defence
OR	Operational Risk
MREL	Minimum Requirements for Own Funds and Eligible Liabilities
O&T RTF	Operational and Technology Risk Type Framework
PRA	Prudential Regulatory Authority
PRT	Principal Risk Type
RA	Risk Appetite
RAS	Risk Appetite Statement
RDAS	Risk Data Aggregation Standards
RCSA	Risk and Control Self-Assessment
RFO	Risk Framework Owner
RRS	Risk Reporting Standards
RTF	Risk Type Framework
SCB	Standard Chartered Bank
SMF	Senior Management Functions
SMR	Senior Managers Regime