42. Bank's Risk Management Approach

Risk management is essential to consistent and sustainable performance for all our stakeholders and is therefore a central part of the financial and operational management of the Group. The Group adds value to clients and to the communities in which they operate, while generating returns for its shareholders by taking and managing risk.

Embedding a healthy risk culture continues to be a core objective across all areas of SCB Group. It underpins an enterprise-level ability to identify and assess, openly discuss, and take prompt action regarding current and future risks.

The Group's Enterprise Risk Management Framework sets out the guiding principles for our staff, enabling us to have integrated and holistic risk conversations across all our principal risks. The Group continues to assess strategic initiatives and growth opportunities from both the financial and non-financial risk perspective, and its approach towards 'effectiveness reviews' facilitates challenge, learning from self-identified issues or weaknesses, and making improvements that are lasting and sustainable.

As part of the Standard Chartered Group, the local Branch is guided by the risk management policies, principles and guidelines set by its Head office and such references made to Group in the ensuing sections, are equally applicable to the local context.

43.1 Risk Management Framework

The Enterprise Risk Management Framework (ERMF) enables the Group to manage enterprise-wide risks, with the objective of maximising risk-adjusted returns while remaining within our Risk Appetite. The ERMF has been designed with the explicit goal of improving the Group's risk management, and since its launch in January 2018, it has been embedded across the Group and rolled out to its branches and subsidiaries.

In 2020, we completed a comprehensive review of the ERMF, and the following changes were approved by the Board:

- Given its overarching nature, Conduct Risk management has been incorporated as an integral component of the overall ERMF rather than viewed as a standalone risk. This change allows the Group to view Conduct Risk through the lens of delivering positive outcomes for our clients, markets, and internal and external stakeholders
- Given the Group's diverse footprint, Country Risk management has also been incorporated as an integral component of the overall ERMF, as part of Group strategy and strategic risk management
- Reputational Risk has been expanded to include Sustainability Risk. There is increasing focus on issues relating to environment, social and governance risk, from both regulators and investors, and the Group's commitments to be a leader in sustainable and responsible banking make this is a core tenet of our franchise
- Technology Risk has been made more prominent within the Operational Risk Principal Risk Type, in order to meet the needs of the digital agenda of the Group and further strengthen Technology Risk management capabilities.

The revised ERMF was approved on 10 December 2020 and became effective on 1 January 2021.

Risk culture

The Group's risk culture provides guiding principles for the behaviours expected from its staff when managing risk. The Board has approved a risk culture statement, applicable to all territories, that encourages the following behaviours and outcomes:

- An enterprise level ability to identify and assess current and future risks, openly discuss these and take prompt actions.
- The highest level of integrity by being transparent and proactive in disclosing and managing all types of risks.
- A constructive and collaborative approach in providing oversight and challenge, and taking decisions in a timely manner.
- Everyone to be accountable for their decisions and feel safe using their judgement to make these considered decisions.

We acknowledge that Banking inherently involves risk-taking and undesired outcomes will occur from time to time; however, we shall take the opportunity to learn from our experience and formalise what we can do to improve. We expect managers to demonstrate a high awareness of risk and control, by self-identifying issues and managing them in a manner that will deliver lasting change.

Roles and responsibilities

Senior Managers Regime

Roles and responsibilities under the ERMF are aligned to the objectives of the Senior Managers Regime. The Group Chief Risk Officer is responsible for the overall development and maintenance of the Group's ERMF and for identifying material risk types to which the Group may be potentially exposed. The Group Chief Risk Officer delegates effective implementation of the Risk Type Frameworks (RTFs) to Risk Framework Owners who provide second line of defence oversight for the Principal Risk Types (PRTs). In addition, the Group Chief Risk Officer has been formally identified as the relevant senior manager responsible for Climate Risk management as it relates to financial and non-financial risks to the Group arising from climate change. This does not include elements of corporate social responsibility, the Group's contribution to climate change and the Sustainable Finance strategy supporting a low-carbon transition, which are the responsibility of other relevant senior managers.

The Risk function

The Risk function is responsible for the sustainability of our business through good management of risk across the Group by providing oversight and challenge, thereby ensuring that business is conducted in line with regulatory expectations. The Group Chief Risk Officer directly manages the Risk function, which is separate and independent from the origination, trading and sales functions of the businesses.

The Risk function is responsible for:

- Maintaining the ERMF, ensuring that it remains relevant and appropriate to the Group's business activities, and is effectively communicated and implemented across the Group, and administering related governance and reporting processes;
- Upholding the overall integrity of the Group's risk and return decisions to ensure that risks are properly assessed, that these decisions are made transparently on the basis of proper assessments and that risks are controlled in accordance with the Group's standards and Risk Appetite; and
- Overseeing and challenging the management of Principal Risk Types under the ERMF.

Three Lines of Defence model

Roles and responsibilities for risk management are defined under a Three Lines of Defence model. Each line of defence has a specific set of responsibilities for risk management and control as shown below.

Lines of Defence	Definition	Key responsibilities include
1st	The businesses and functions engaged in or supporting revenue generating activities that own and manage risks	• Identify, monitor and escalate risks and issues to the Second Line and senior management1 and promote a healthy risk culture and good conduct • Manage risks within Risk Appetite and ensure laws and regulations are being complied with • Ensure systems meet risk data aggregation, risk reporting and data quality requirements set by the Second Line
2nd	The control functions independent of the First Line that provides oversight and challenge of risk management to provide confidence to the Group Chief Risk Officer, the management team and the Board.	• Identify, monitor and escalate risks and issues to the Group Chief Risk Officer, senior management and the Board and promote a healthy risk culture and good conduct • Oversee and challenge First Line risk taking activities and review First Line risk proposals • Propose Risk Appetite to the Board, monitor and report adherence to Risk Appetite and intervene to curtail business if it is not in line with existing or adjusted Risk Appetite • Set risk data aggregation, risk reporting and data quality requirements
3rd	The independent assurance provided by the Group Internal Audit Function, of the effectiveness of controls that support First Line's risk management of business activities, and the processes maintained by the Second Line. Its role is defined and overseen by the Audit Committee of the Board.	• Independently assess whether management has identified the key risks in the business and whether these are reported and governed in line with the established risk management processes • Independently assess the adequacy of the design of controls and their operating effectiveness

The Country Risk Committee, the Country Financial Crime Risk Committee and the Country Asset and Liability Committee are responsible for ensuring that our risk profile is managed in compliance with the Risk Appetite set by the Board. The Board Risk Committee and the Board Financial Crime Risk Committee (for Financial Crime Compliance) advise the Board on the Risk Appetite Statement and monitor the compliance of the same.

Risk Appetite and profile

The Group recognises the following constraints which determine the risks that it is willing to take in pursuit of its strategy and the development of a sustainable business:

Risk capacity is the maximum level of risk the Group can assume, given its current capabilities and resources, before breaching constraints determined by capital and liquidity requirements and internal operational capability (including but not limited to technical infrastructure, risk management capabilities, expertise), or otherwise failing to meet the expectations of regulators and law enforcement agencies.

Risk Appetite is defined by the Group and approved by the Board. It is the maximum amount and type of risk the Group is willing to assume in pursuit of its strategy. Risk Appetite cannot exceed risk capacity The Board has approved a Risk Appetite Statement, which is underpinned by a set of financial and operational control parameters known as Risk Appetite metrics and associated thresholds.

These directly constrain the aggregate risk exposures that can be taken across the Group. The Risk Appetite Statement is supplemented by an overarching statement outlining the Group's Risk Appetite Principles.

Risk Appetite Principles

The Group Risk Appetite is defined in accordance with risk management principles that inform our overall approach to risk management and our risk culture. We follow the highest ethical standards required by our stakeholders and ensure a fair outcome for our clients, as well as facilitating the effective operation of financial markets, while at the same time meeting expectations of regulators and law enforcement agencies. We set our Risk Appetite to enable us to grow sustainably and to avoid shocks to earnings or our general financial health, as well as manage our Reputational Risk in a way that does not materially undermine the confidence of our investors and all internal and external stakeholders.

Risk Appetite Statement

The Group will not compromise adherence to its Risk Appetite in order to pursue revenue growth or higher returns. To keep the Group's Risk profile within Risk Appetite (and therefore also risk capacity), we have cascaded critical Group Risk Appetite metrics across our Principal Risk Types to countries with significant business operations. These are supplemented by risk control tools such as granular level limits, policies, standards and other operational control parameters that are used to keep the Group's risk profile within Risk Appetite. The Group's risk profile is its overall exposure to risk at a given point in time, covering all applicable risk types. Status against Risk Appetite is reported to the Board Risk Committee and the Group Risk Committee, including the status of breaches and remediation plans here applicable. Country Risk Appetite is managed at a country level with Group and regional oversight.

The Group Risk Committee, the Group Financial Crime Risk Committee, the Group Non-Financial Risk Committee and the Group Asset and Liability Committee are responsible for ensuring that our risk profile is managed in compliance with the Risk Appetite set by the Board.

The Board Risk Committee and the Board Financial Crime Risk Committee (for Financial Crime Compliance) advise the Board on the Risk Appetite Statement and monitor the Group's compliance with it.

At a country level, the appetite for each type of risk is addressed in relation to the country's business strategy while reviewing: Credit Approval Documents ("CAD"), Corporate Portfolio Standards, Product Programmes and Country Addendums, the Integrated Risk Management Framework (IRMF), country limits for transaction types and risk measurement metrics.

Risk identification and assessment

Identification and assessment of potential adverse risk events is an essential first step in managing the risks of any business or activity. To ensure consistency in communication we use Principal Risk Types to classify our risk exposures.

Nevertheless, we also recognise the need to maintain an overall perspective since a single transaction or activity may give rise to multiple types of risk exposure, risk concentrations may arise from multiple exposures that are closely correlated, and a given risk exposure may change its form from one risk type to another.

Principal Risk Types

Principal risks are those risks that are inherent in our strategy and our business model. These risks are managed through distinct Risk Type Frameworks (RTF). The RTFs are approved by the Group Chief Risk Officer. The principal risks and associated Risk Appetite Statements are approved by the Board. As part of the overall risk management framework review in 2018, we also reviewed our Principal Risk Types. The table below shows the current Group's principal risks.

Principal Risk Types	Definitions	How these are managed
Credit risk	Potential for loss due to the failure of a counterparty to meet its agreed obligations to pay the Group	The Group manages its credit exposures following the principle of diversification across products, geographies, client segments and industry sectors
Traded risk	Potential for loss resulting from activities undertaken by the Group in financial markets	The Group controls its trading portfolio and activities to ensure that traded risk losses (financial or reputational) do not cause material damage to the Group's franchise
Capital & Liquidity risk	Capital: Potential for insufficient level, composition or distribution of capital to support our normal activities Liquidity: potential for loss where we may not have sufficient stable or diverse sources of funding or financial resources to meet our obligations as they fall due	The Group maintains a strong capital position, including the maintenance of management buffers sufficient to support its strategic aims, and holds an adequate buffer of high-quality liquid assets to survive extreme but plausible liquidity stress scenarios for at least 60 days without recourse to extraordinary central bank support
Operational and technology risk	Potential for loss resulting from inadequate or failed internal processes and systems, human error, or from the impact of external events (including legal risks)	The Group controls operational 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	Potential for loss from a breach of confidentiality, integrity and availability of the Group's information systems and assets through cyber-attack, insider activity, error or control failure	The Group seeks to avoid risk and uncertainty for our critical information assets and systems and has a low appetite for material incidents affecting these or the wider operations and reputation of the bank
Compliance risk	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	The Group has no appetite for breaches in laws and regulations, while recognising that while regulatory non-compliance cannot be entirely avoided, the Group strives to reduce this to an absolute minimum
Financial Crime risk	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, anti-bribery and corruption, and fraud	The Group has no appetite for breaches in laws and regulations related to financial crime, recognising that while incidents are unwanted, they cannot be entirely avoided
Reputational and Sustainability risk	Potential for damage to the franchise, resulting in loss of earnings or adverse impact on market capitalisation because of stakeholders taking a negative view of the organisation, its actions or inactions, including a failure to uphold responsible business conduct or lapses in our commitment to do no significant environmental and social harm through our client, third-party relationships, or our own operations	The Group protects the franchise from material damage to its reputation by ensuring that any business activity is satisfactorily assessed and managed by the appropriate level of management and governance oversight
Model risk	Potential loss that may occur as a consequence 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	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 model uncertainty

In 2020, a comprehensive review of the Group ERMF was completed and the following key changes were approved by the Board:

- Given its overarching nature, Conduct Risk Management has been incorporated as an integral component of the overall ERMF rather than viewed as a standalone risk. This change allows the Group to view Conduct Risk through the lens of delivering positive outcomes for our clients, markets, and internal and external stakeholders
- Given the Group's diverse footprint, Country Risk management has also been incorporated as an integral component of the overall ERMF, as part of Group strategy and strategic risk management
- Reputational Risk has been expanded to include Sustainability Risk. There is increasing focus on issues relating to environment, social and governance risk from both regulators and investors, and the Group's commitments to be a leader in sustainable and responsible banking make this is a core tenet of our franchise
- Technology risk has been made more prominent within the Operational Risk principal risk type, in order to meet the needs of the digital agenda of the Group and further strengthen Technology risk management capabilities

The revised ERMF was approved on 10 December 2020 and became effective on 1 January 2021.

In Sri Lanka too, the same philosophy of risk management is replicated in a manner relevant to the local organisation structure of the Branch.

Risk and Compliance function

The Group Chief Risk Officer directly manages the Risk and Compliance function that is separate and independent from the origination, trading and sales functions of the businesses. The role of the function is:

- To maintain the Enterprise Risk Management Framework, ensuring it remains appropriate to the Group's activities, is effectively communicated and implemented across the Group, and to administer related governance and reporting processes.

- To uphold the overall integrity of the Group's risk/return decisions, and in particular to ensure that risks are properly assessed, that risk/return decisions are made transparently on the basis of this proper assessment, and that risks are controlled in accordance with the Group's standards and Risk Appetite.

- To oversee and challenge the management of credit, country, market, operational, reputational, compliance, conduct, information and cyber security and financial crime risk types. The independence of the Risk and Compliance function is to ensure that the necessary balance in risk/return decisions is not compromised by short-term pressures to generate revenues.

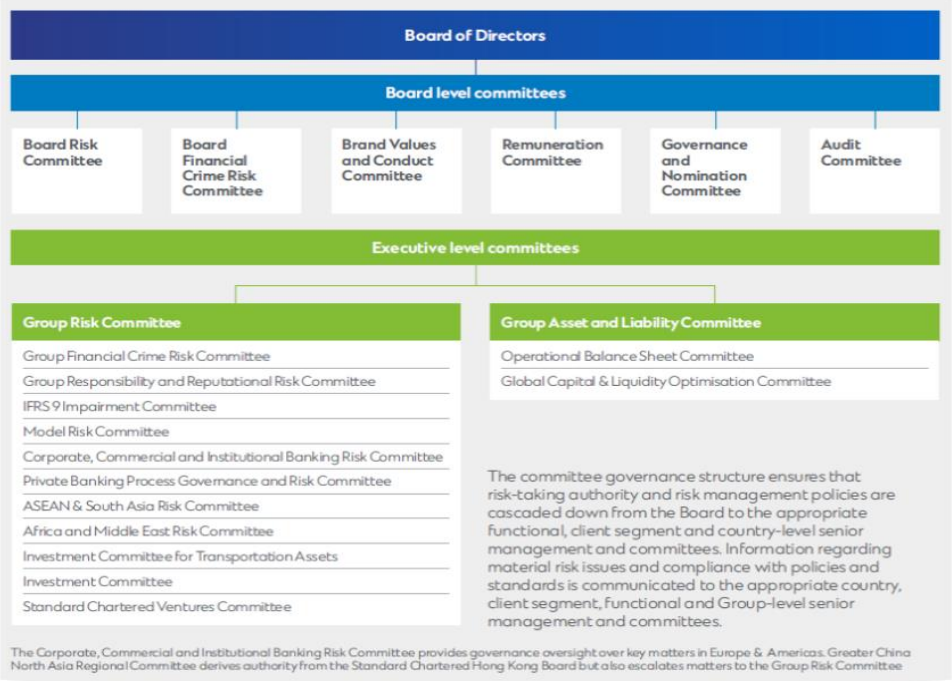
Locally, the Compliance function is led by the Head of Compliance, whilst the Risk function is managed by the Chief Risk Officer.

43.2 General Governance

The committee governance structure ensures that risk-taking authority and risk management policies are cascaded down from the Board through to the appropriate functional, client business and country-level senior management and committees.

Information regarding material risk issues and compliance with policies and standards is communicated to the appropriate country, client business, functional and Group-level senior management and committees.

The following diagram depicts the Group's governance structure:



The Branch's committee governance structure ensures that risk-taking authority and risk management policies are cascaded down from Group Asset & Liability Committee (GALCO) and Group Chief Risk Officer (GCRO) to the appropriate functional and divisional committees. Information regarding material risk issues and compliance with policies and standards is communicated through the business and functional committees up to the Group-level committees, as appropriate.

The Country Management Team (CMT) drives and executes the business and governance agenda bringing alignment across the business and the functions to maximise and protect the value of the Group's operations in Sri Lanka. The CMT is comprised of the senior executive members of the Branch. However, the Asset & Liability Committee (ALCO) and Country Risk Committee (CRC) are the senior approving committees of the Branch. Their responsibilities and membership are outlined in the table below.

Committee	Membership	Purpose
ALCO	– Chief Executive Officer [CEO] (Chair) – Financial Controller (Alternate Chair) – Chief Country Risk Officer (CCRO) *(Besides, the permanent members stated above, representatives from CCIB, CPBB, Treasury Markets, Financial Markets, Market Risk and Treasury Risk are represented at this forum on a permanent invitee basis)*	Responsible for the management of Capital and Liquidity; the establishment and compliance with policies relating to Balance Sheet Management, including the management of the Bank's Capital Adequacy; and approval of the Bank's ICAAP document. Meeting frequency: At least ten times per annum.
CRC	– CCRO (Chair) – CEO (Alternate Chair) – Head of Local and International Corporates – Head, CPBB – Head, Conduct Financial Crime and Compliance – Chief Operating Officer – Financial Controller – Head of Legal – Head of Human Resources – Director Financial Crime Compliance and Country Money Laundering Compliance Officer – Information Security Risk Officer (ISRO) India & Cluster – Head Risk and Controls – ITO & HICS (First line for ICS)	Responsible for the management of all risks, except those for which ALCO has direct responsibility. To oversee the overall risk management framework and effective implementation of Risk Type Framework in SCB Sri Lanka and its effective application in Country and approval of the stress scenario and stress testing results of the ICAAP. Meeting Frequency: At least six times per annum.

43.3 Credit risk

Credit risk is the potential for loss due to the failure of a counterparty to meet its obligations to pay the Group in accordance with agreed terms. Credit exposures arise from both the banking and trading books.

Credit Risk, which is a Principal Risk is managed through a Risk Type Framework that sets out policies and procedures covering the measurement and management of credit risk. There is a clear segregation of duties between transaction originators in the businesses and approvers in the Risk function. All credit exposure limits are approved within a defined credit approval authority framework.

The Group manages its credit exposures following the principle of diversification across products, geographies, industries, collateral types and client segments.

Credit Risk Governance

The Country Risk Committee (CRC) and the Credit Issues Committee (CIC) are responsible for overseeing the credit risk profile of the portfolios. Meetings are held regularly, and the Committees monitor credit risk portfolios, key internal developments and external trends, and ensure that appropriate action is taken.

In addition, there are other Group-wide policies integral to credit risk management such as those relating to stress testing, risk measurement and impairment provisioning. Policies and procedures specific to each client or product segment are established by authorised bodies. These are consistent with our Group-wide credit policies but are more detailed and adapted to reflect the different risk characteristics across client and product segments. Policies are regularly reviewed and monitored to ensure these remain effective and consistent with the risk environment and risk appetite.

Credit policies

Credit policies and standards are considered and approved by recognised second line risk committees or individuals with delegated authority. The Group Risk Committee oversees the delegation of credit approval and loan impairment provisioning authorities. The principles for the delegation, review and maintenance of credit approval authorities are defined in the Risk Authorities policy. In addition, there are other Group-wide policies integral to credit risk management such as those relating to stress testing, risk measurement and impairment provisioning.

Credit rating and measurement

Risk measurement plays a central role, along with judgement and experience, in informing risk-taking and portfolio management decisions.

A standard alphanumeric Credit Risk grade system is used for Corporate & Institutional Banking and Commercial Banking. The numeric grades run from 1 to 14 and some of the grades are further sub-classified. Lower numeric credit grades are indicative of a lower likelihood of default. Credit grades 1 to 12 are assigned to performing customers, while credit grades 13 and 14 are assigned to non-performing or defaulted customers.

Retail Banking internal ratings-based portfolios use application and behavioural credit scores that are calibrated to generate a probability of default.

Credit approval and credit risk assessment

The Credit Risk Type Frameworks are the formal mechanism which delegate Credit Risk authorities cascading from the Group Chief Risk Officer, as the Senior Manager of the Credit Risk Type, to individuals such as the business segments' Chief Risk Officers. Named individuals further delegate credit authorities to individual credit officers by applying delegated credit authority matrices, which determine the maximum limits based on risk-adjusted scales by customer type or portfolio. Credit Risk authorities are reviewed at least annually to ensure that they remain appropriate. In Corporate & Institutional Banking, Commercial Banking, the individuals delegating the Credit Risk authorities perform oversight by reviewing a sample of the limit applications approved by the delegated credit officers on a monthly basis. In Retail Banking, credit decision systems and tools (e.g., application scorecards) are used for credit decision making. Where manual credit decisions are applied, these are subject to periodic quality control assessment and assurance checks.

All other credit approval authorities are delegated by the Group Risk Committee to individuals based both on their judgement and experience and a risk-adjusted scale that takes account of the estimated maximum potential loss from a given customer or portfolio. Credit origination and approval roles are segregated in all, but a very few authorised cases for Retail Clients. In those very few exceptions where they are not, originators can only approve limited exposures within defined risk parameters, which are subject to oversight from the credit risk function.

All credit proposals are subject to a robust credit risk assessment. It includes a comprehensive evaluation of the client's credit quality, including willingness, ability and capacity to repay. The primary lending consideration is usually based on the client's credit quality and the repayment capacity from operating cash flows for counterparties; and personal income or wealth for individual borrowers. The risk assessment gives due consideration to the client's liquidity and leverage position.

Where applicable, the assessment includes a detailed analysis of the credit risk mitigation arrangements to determine the level of reliance on such arrangements as the secondary source of repayment in the event of a significant deterioration in a client's credit quality leading to default. Lending activities that are considered as higher risk or non-standard are subjected to stricter minimum requirements and require escalation to a senior credit officer or authorised bodies.

Credit risk mitigation

Potential credit losses from any given account, client or portfolio are mitigated using a range of tools such as collateral, netting agreements, credit insurance and guarantees. The reliance that can be placed on these mitigants is carefully assessed in light of issues such as legal certainty and enforceability, market valuation correlation and counterparty risk of the guarantor.

The Group credit risk mitigation policy determines the key considerations for eligibility, enforceability and effectiveness of credit risk mitigation arrangements. The Group has policies and procedures in place (which are followed by the Branch) setting out the criteria for collateral to be recognised as a credit risk mitigant, including requirements concerning legal certainty, priority, concentration, correlation, liquidity and valuation parameters such as frequency of review and independence.

Collateral types that are eligible for risk mitigation include: cash; residential, commercial and industrial property; fixed assets such as motor vehicles, plant and machinery; marketable securities; commodities; bank guarantees; and letters of credit. The Group also enters into collateralised reverse repurchase agreements.

In order to be recognised as security and for the loan to be classified as secured, all items pledged must be valued independently and an active secondary resale market for the collateral must exist. Documentation must be held to enable the Bank to realise the asset without the cooperation of the asset owner if this is necessary. The Bank also seeks to diversify its collateral holdings across asset classes and markets.

For certain types of lending, typically mortgages or asset financing where a first charge over the risk mitigant must be attained, the right to take charge over physical assets is significant in terms of determining appropriate pricing and recoverability in the event of default. The requirement for collateral is, however, not a substitute for the ability to pay, which is the primary consideration for any lending decisions.

Regular valuation of collateral is required in accordance with the Group's credit risk mitigation policy, which prescribes both the process of valuation and the frequency of valuation for different collateral types. The collateral must be independently valued prior to drawdown and regularly thereafter. The valuation frequency is typically annual and more frequent valuations are driven by the level of price volatility of each type of collateral and the nature of the underlying product or risk exposure. Risk mitigation benefits may be removed where the collateral value is not supported by a recent independent valuation.

For financial collateral to be eligible for recognition, the risk mitigant relied upon must be sufficiently liquid and its value over time sufficiently stable to provide appropriate certainty as to the credit protection achieved. Stress tests are performed on changes in collateral values for key portfolios to assist senior management in managing the risks in those portfolios.

Physical collateral is required to be insured at all times against risk of physical loss or damage; insurance for other risks is kept under review.

Collateral values are, where appropriate, adjusted to reflect current market conditions, the probability of recovery and the period to realise the collateral in the event of possession. Where guarantees or credit derivatives are used as credit risk mitigation, the creditworthiness of the guarantor is assessed and established using the credit approval process in addition to that of the obligor or main counterparty. The main types of guarantors include banks, insurance companies, parent companies, shareholders and export credit agencies.

Credit monitoring

We regularly monitor credit exposures, portfolio performance, and external trends that may impact risk management outcomes. Internal risk management reports are presented to risk committees, containing information on key environmental, political and economic trends across major portfolios and countries; portfolio delinquency and loan impairment performance; and IRB portfolio metrics including credit grade migration.

In Corporate & Institutional Banking and Commercial Banking, clients and portfolios are subjected to additional review when they display signs of actual or potential weakness; for example, where there is a decline in the client's position within the industry, financial deterioration, a breach of covenants, or non-performance of an obligation within the stipulated period. Such accounts are subjected to a dedicated process overseen by the Credit Issues Committees in country, where client account strategies and credit grades are re-evaluated. In addition, remedial actions including exposure reduction, security enhancement, or exiting the account could be undertaken, and certain accounts could also be transferred into the control of Group Special Assets Management (GSAM), which is our specialist recovery unit for Corporate & Institutional Banking and Commercial Banking, that operates independently from our main business. For Retail Banking exposures, portfolio delinquency trends are monitored on an ongoing basis. Account monitoring is based on behaviour scores and bureau performance (where available). Accounts that are past due (or perceived as high risk and not yet past due) are subject to a collections or recovery process managed by a specialist function independent from the origination function.

Credit concentration risk

Credit concentration risk may arise from a single large exposure to a counterparty or a group of connected counterparties, or from multiple exposures across the portfolio that are closely correlated. Large exposure concentration risk is managed through concentration limits set by counterparty or group of connected counterparties.

At the portfolio level, credit concentration thresholds are set and monitored to control concentrations, where appropriate, by industry, product, tenor, collateral type, collateralization level, exposure to holding companies and credit risk profile.

For concentrations that are material at a Group level, thresholds are set and monitored by the respective governance committees and reported to the Group Risk and Board Risk Committees. Locally, credit concentrations are monitored by the Country Risk Committee against internal 'Portfolio Standards' as well as the regulatory thresholds imposed by the SBL (Single Borrower Limit).

Industry and product concentration of the customer portfolio as at 31.12.20:

Industry Sector	% of Exposure*
Manufacturing	44%
Trading	12%
Agriculture and fishing	11%
Transport	5%
Financial and Business Services	1%
Infrastructure	8%
Construction	3%
Other Customers (incl. Retail Clients)	16%
Total	**100%**

Product Category	% of Exposure*
Overdrafts	18%
Trade finance	20%
Credit cards	8%
Staff loans	1%
Personal Loans	11%
Corporate Loans	42%
Total	**100%**

* As a percentage of total customer loans and advances portfolio.

Credit quality analysis

The table below set out the loan portfolio and the impairment provisions held based on SLFRS 9.

As at 31st December 2020	(Rs. '000)
Loans and Receivables – Performing	80,585,394
Loans and Receivables – Non-Performing	2,511,163
Total Loans and Receivables	**83,096,556**
Less: Expected Credit Loss (Stages 1)	(449,804)
Less: Expected Credit Loss (Stages 2)	(234,360)
Less: Expected Credit Loss (Stages 3)	(1,256,248)
Net Loans and Receivables	**81,156,144**

43.4 Traded Risk

Under the Enterprise Risk Management Framework, the introduction of the Traded Risk Type Framework (TRTF) sought to bring together all risk types exhibiting risk features common to Traded Risk. Traded Risk Management (TRM) is the core risk management function supporting market facing businesses, specifically Financial Markets and Treasury Markets.

Roles and responsibilities

The TRTF, which sets the roles and responsibilities in respect of Traded Risk for the Group, is owned by the Global Head, Traded Risk Management. The front office, acting as first line of defence, are responsible for the effective management of risks within the scope of its direct organizational responsibilities set by the Board. The TRM function is the second line control function that performs independent challenge, monitoring and oversight of the Traded Risk management practices of the first line of defence. The first and second lines of defence are supported by the organization structure, job descriptions and authorities delegated by Traded Risk control owners.

The Branch recognizes market risk as the potential for loss of earnings or economic value due to adverse changes in financial market rates or prices. The Branch is exposed to market risk arising principally from customer-driven transactions. The objective of the Branch's market risk policies and processes is to obtain the best balance of risk and return while meeting customers' requirements. The primary categories of market risk for the Group/Branch are interest rate risk and currency exchange.

Traded risk governance

The Group's Risk Appetite Statement, along with the key associated Risk Appetite metrics, is approved by the Board with responsibility for Traded Risk limits, then tiered accordingly.

Subject to the Group's Risk Appetite for Traded Risk, the limits are approved by the TRM and CRC for the Branch. Additional limits are placed on specific instruments, positions, and portfolio concentrations where appropriate. Authorities are reviewed at least annually to ensure they remain appropriate and to assess the quality of decisions taken by the authorized person. Key risk-taking decisions are made only by certain individuals with the skills, judgement and perspective to ensure that the Group's control standards and risk-return objectives are met. Authority delegators are responsible for monitoring the quality of the risk decisions taken by their delegates and the ongoing suitability of their authorities.

Foreign Exchange Exposure

The foreign exchange exposures comprise trading and non-trading foreign currency translation exposures. Foreign exchange trading exposures are principally derived from customer driven transactions.

Interest Rate Exposure

The interest rate exposures arise from trading and non-trading activities. Structural interest rate risk arises from the differing re-pricing characteristics of commercial banking assets and liabilities.

The Bank uses the following techniques to manage the market risk arising due to foreign exchange and the interest rate exposures.

a. Value at Risk

The Branch measures the risk of losses arising from future potential adverse movements in market rates, prices and volatilities using a VaR methodology. VaR, in general, is a quantitative measure of market risk that applies recent historical market conditions to estimate the potential future loss in market value that will not be exceeded in a set time period at a set statistical confidence level. VaR provides a consistent measure that can be applied across trading businesses and products over time and can be set against actual daily trading profit and loss outcome.

VaR is calculated for expected movements over a minimum of one business day and to a confidence level of 97.5 per cent. This confidence level suggests that potential daily losses, in excess of the VaR measure, are likely to be experienced six times per year. To assess their ongoing performance, VaR models are back-tested in the Group against actual results.

b.Market Risk Changes

Daily value at risk (VaR at 97.5%, one day)

By Risk Type (All in Rs. 000's)	2020			
	Highest	Lowest	Average	31st Dec
FX Risk – Trading	29,174	6,585	15,440	6,634
Interest Rate Risk – Non-Trading	38,268	10,558	17,431	13,030

By Risk Type (All in Rs. 000's)	2019			
	Highest	Lowest	Average	31st Dec
All – Trading	14,960	1,260	6,924	4,121
Interest Rate Risk – Non Trading	57,068	14,919	30,456	22,114

Interest Rate Risk in the Banking Book

Interest rate risk from across the non-trading book portfolios is transferred to the Treasury Markets (TM) desk where it is managed under the supervision of ALCO. The TM desk deals in the market in approved financial instruments in order to manage the net interest rate risk, subject to approved VaR and risk limits.

Losses beyond the 97.5 per cent confidence interval are not captured by a VaR calculation, which therefore gives no indication of the size of losses in tail event situations. TRM complements the VaR measurement by regular stress testing of market risk exposures to highlight the potential risk that may arise from extreme market events that are rare but plausible. VaR and stress tests are applied to non-trading book exposures in the same way as for the trading book.

The country Asset and Liability Committees (ALCO) are responsible for any residual interest rate risks that cannot be managed by TM.

Stress testing

Stress testing is an integral part of the market risk management framework and considers both, historical market events and forward-looking scenarios. A consistent stress testing methodology is applied to trading and non-trading books. The stress testing methodology assumes that scope for management action would be limited during a stress event, reflecting the decrease in market liquidity that often occurs. Stress scenarios are regularly updated to reflect changes in risk profile and economic events.

Regular stress test scenarios are applied to interest rates, credit spreads and exchange rates thereby covering asset classes in the FM and TM non-trading and trading books. Ad hoc scenarios are also prepared reflecting specific market conditions and for particular concentrations of risk that arise within the businesses.

43.5 Capital Risk and Liquidity Risk

The Group expects to maintain a strong capital position including the maintenance of management buffers sufficient to support its strategic aims and hold an adequately stable or diverse source of funding or financial resources to meet our obligations as they fall due.

Liquidity risk and funding risk

Liquidity risk and Funding Risk is the potential for loss where we may not have sufficient stable or diverse sources of funding or financial resources to meet our obligations as they fall due. The Liquidity Risk Framework governs liquidity risk and the oversight is maintained by ALCO. In accordance with the framework, the Branch maintains a liquid portfolio of marketable securities as reserve assets. The level of the Branch's aggregate liquid reserves is in accordance with local regulatory minimum liquidity requirements.

Funding risk is the potential for actual or opportunity loss because the Branch does not have stable or diversified sources of funding in the medium and long-term to enable it to meet its financial obligations, in pursuit of its desired business strategy or growth objectives.

At a country level, the Financial Controller is the risk framework owner for liquidity risk and operationally Treasury Markets, Finance and the Treasury Risk representative, working in collaboration are responsible for implementing the Liquidity Risk Type Framework.

The Bank expects to manage its liquidity and funding prudently for all currencies. Exceptional market events could impact us adversely, thereby potentially affecting our ability to fulfill our obligations as they fall due.

To mitigate liquidity and funding risks the Bank has access to wholesale funds under normal market conditions. The Bank maintains a significant portfolio of marketable securities that can be monetized or pledged as collateral in the event of a liquidity stress. The Liquidity Contingency Plan, reviewed and approved quarterly, is maintained by Finance. It includes an escalation framework and a set of management actions that could be effectively implemented in the event of a liquidity stress.

Maturity Analysis

The Branch prepares a Maturities of Assets and Liabilities based on contractual residual maturities. This analysis however, does not consider the core proportion of customer assets and deposits which remain with the Branch on a rollover/revolving basis. As such, based on empirical data, core balance percentages are derived and applied to forecast the 'most likely' expected cash flows, referred to as the Maximum Cumulative Outflow (MCO) analysis, which is calculated daily and monitored against pre-set limits.

Stress Scenarios

The branch conducts two (02) tests routinely: (a) an acute 8-day name specific stress test, and (b) a 90-day market wide stress test.

The 8-day stress test is performed weekly. This is intended to ensure that, in the unlikely event of an acute loss of confidence in the Group or the Branch, there is sufficient time to take corrective action.

The resilience to unexpected local market disruptions (e.g. interbank money or foreign exchange markets) is tested by a 90-day market wide stress test performed daily. Every country must pass these two tests on a stand-alone basis.

Liquidity metrics

The Branch monitors the liquidity position (on a pan-Bank basis) using key liquidity metrics on a regular basis, which includes both internal measures and those required by the Central Bank of Sri Lanka.

Advances-to-Deposits Ratio (ADR)	**2020**		**2019**	
	LCY*	**FCY***	**LCY**	**FCY**
Year-end	54%	60%	103%	84%
Maximum	110%	100%	105%	116%
Minimum	47%	58%	76%	71%
Average	76%	75%	89%	85%

*LCY – Local currency FCY – Foreign currency

Other Liquidity Monitoring Metrics	**2019 Dec.**	**2020 March**	**2020 June**	**2020 Sept.**	**2020 Dec.**	**Min. Requirement**
Liquid Asset Ratio - DBU (%)	62%	63%	62%	89%	83%	20%
Liquid Asset Ratio - FCBU (%)	52%	52%	44%	39%	56%	20%
Liquidity Coverage Ratio (LCR) – All Currency	180%	247%	294%	317%	354%	100%
Liquidity Coverage Ratio (LCR) – LKR	176%	309%	446%	421%	597%	100%
Medium Term Funding (MTF) Ratio - LCY (%) *	329%	324%	351%	473%	454%	**50%
Medium Term Funding (MTF) Ratio - FCY (%) *	154%	194%	232%	175%	101%	**50%
Net Stable Funding Ratio (NSFR)	467%	537%	628%	596%	487%	100%

* Medium Term Funding (MTF) Ratio: The MTF ratio is an internal ratio used to evaluate the coverage of assets with a contractual maturity of more

than 1 year by funding sources with a contractual maturity of more than 1 year. The ratio is calculated for Local Currency (LCY) and Foreign Currency (FCY) assets and liabilities separately.
** Internal Management Action Trigger.

Sensitivity of Assets and Liabilities (SAL)

The interest rate sensitivity profile of assets and liabilities prepared as per the guidelines provided in the Integrated Risk Management Framework (IRMF) is provided in Disclosure 6.

Capital Risk

The Group defines Capital Risk as the potential for insufficient level, composition or distribution of capital to support our normal activities. The Financial Controller is the risk type owner for capital risk, which is managed through the ALCO.

Capital planning

On an annual basis, strategic business and capital plans are drawn up covering a five-year horizon and are approved by the CMT. The capital plan ensures that adequate levels of capital, including loss absorbing capacity, and an efficient mix of the different components of capital are maintained to support our strategy and business plans.

Capital planning takes the following into account:

- Current regulatory capital requirements and our assessment of future standards and how these might change
- Demand for capital due to the business and loan impairment outlook and potential market shocks or stresses
- Available supply of capital and capital raising options, including ongoing capital accretion from the business

Capital Maintenance

Pillar I – Minimum capital ratio maintenance: Pillar I capital requirements measure the Bank's adequacy of capital in relation to three main categories of risk – i.e. credit risk, market risk and operational risk. The Branch is well capitalized as reflected by the Capital Adequacy Ratios depicted below.

	31.12.2020*	**31.12.2019***	**Min. Requirement**
CET 1 Ratio	17.28%	18.33%	7.00%
Tier 1 Capital Ratio	17.28%	18.33%	8.50%
Total Capital Ratio	17.81%	18.64%	12.50%
Leverage Ratio (w.e.f. 01.01.2019)	10.89%	13.81%	3.00%

* Inclusive of certified profits of the financial year then ended.

The Central Bank of Sri Lanka announced a temporary relief (following the Covid-19 pandemic), by reducing the minimum capital requirement by 50bps, till 30th June 2021.

Pillar II - Internal Capital Adequacy Assessment Process (ICAAP)

The ICAAP process evaluates the Branch's resilience under stressed conditions. Stress testing and scenario analysis are used to assess the Branch's ability to maintain operations (consistent with its risk appetite) during a period of severe but plausible stress conditions, and to simulate a set of feasible management actions and their impact on the Branch's earning, risk profile and capital position, should such conditions materialize. These conditions may arise from economic, liquidity, legal, political or physical events, or from materialization of risks that are unique to the Branch, which are evaluated under Pillar 2.

The Branch submitted its 2020 ICAAP to the Central Bank of Sri Lanka on 30th June 2020. Based on the evaluation performed, it indicated that the Branch was able to meet the minimum capital requirements during the 5-years simulated for the stress testing exercise, which assumed an economic downturn with a severity of 1 in 25 years.

Stress testing and Sensitivity analysis

Stress testing and scenario analysis are an integral part of the capital and liquidity framework and are used to ensure that the Group's internal assessment of capital and liquidity considers the impact of extreme but plausible scenarios on its risk profile. They provide an insight into the potential impact of significant adverse events on the Group's capital and liquidity position and how this could be mitigated through appropriate management actions to ensure the Group remains within the approved Risk Appetite and regulatory limits.

Our approach to stress testing is designed to:

- Identify key risks to our capital and liquidity positions, strategy, franchise and reputation
- Support the development of strategic management actions and contingency plans, including business continuity, to ensure the Branch can recover from extreme but plausible conditions
- Meet country regulatory requirements

43.6 Operational and Technological Risk

Overview

We define operational risk as the potential for loss from inadequate or failed internal processes and systems, human error or from the impact of external events, including legal risks. The management of operational risk is a challenge due to its broad scope as operational risks arise from all activities carried out within the Banks. To address this challenge, we map risks across the Group at a processes level with controls installed to mitigate these risks.

Three Lines of Defence

To implement its operational risk management approach, the Group applies the Three Lines of Defence model, as set out in the Enterprise Risk Management Framework. Each line of defence has a specific set of responsibilities for risk management and control as follows:

- The first line of defence is responsible for identifying and managing the inherent risks in processes they own.
- The second line of defence is responsible for setting and maintaining control standards for the operational risk management. The second line of defence comprises both risk owners of each operational risk sub-type and Group policy owners.
- The third line of defence is the independent assurance provided by the Group Internal Audit function.

Managing Operational Risk

Roles and responsibilities

The Operational Risk Type Framework (ORTF) is set by the Global Head of Risk, Functions and Operational Risk and is applicable enterprise-wide. This Framework defines and collectively groups operational risks which have not been classified as principal risks into non-Principal Risk Types (non-PRTs) and sets standards for the identification, control, monitoring and treatment of risks. These standards are applicable across all PRTs and non-PRTs. The non-PRTs relate to execution capability, governance, reporting and obligations, legal enforceability, and operational resilience (including client service, third party vendor services, change management, safety and security and system availability). The ORTF reinforces clear accountability for managing risk throughout the Group and delegates second line of defence responsibilities to identified subject matter experts. For each non-PRT, the expert sets policies for the organisation to comply with, and provides guidance, oversight and challenge over the activities of the Group. They 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.

Mitigation

The ORTF sets out the Group's overall approach to the management of Operational Risk in line with the Group's Operational Risk Appetite. This is supported by Control Assessment Standards (CAS) which define roles and responsibilities for the identification, control and monitoring of risks (applicable to all non-PRTs and PRTs). The CAS are used to determine the design strength and reliability of each process, and require:

- The recording of processes run by client segments, products, and functions into a process universe
- The identification of potential breakdowns to these processes and the related risks of such breakdowns
- An assessment of the impact of the identified risks based on a consistent scale;
- The design and monitoring of controls to mitigate prioritised risks
- Assessments of residual risk and timely actions for elevated risks

Risks that exceed the Group's thresholds require treatment plans to address underlying causes.

Governance Committee Oversight

At the Board level, the Board Risk Committee oversees the effective management of Operational risk. At the executive level, the Group Risk Committee delegates authority primarily to the Group Non-Financial Risk Committee (GNFRC) to monitor the Group's Operational Risk Appetite and to oversee the Group's Operational risk profile.

The GNFRC has the authority to challenge, constrain and, if required, stop business activities where risks are not aligned with the Group's Operational Risk Appetite.

Regional, business segment and functional committees, also provide enterprise oversight of their respective processes and related operational risks. In addition, Country Non-Financial Risk Committees (CNFRCs) oversee the management of Operational risks at the country (or entity) level. In Sri Lanka, the responsibilities of the CNFRC are exercised directly by the Country Risk Committee (CRC).

Business Continuity Management

Business Continuity Management (BCM) is the planning and preparation for continuity of critical business operations and infrastructure to ensure their ongoing availability in the event of any significant business interruption. There are three disciplines under BCM which are Crisis Management, Business Continuity Planning (BCP), and IT Disaster Recovery (IT DR). Crisis Management governs the manner in which the Branch responds to control a crisis. BCP and IT DR create and manage our predetermined responses to a crisis, enabling us to mitigate impact from significant business interruption.

The Branch has seven identified recovery solutions that can be implemented for a robust recovery strategy. (Split Operations, use of common office areas, Working From Home (WFH), host / Refugee, cross Border transfer of activities, dedicated BCP seats - Leased or owned properties, dedicated BCP seats - Vendor Contract).

The Branch's disaster recovery site which is situated at Malabe is fully equipped with all the infrastructure facilities, Information technology equipment and communication facilities. All the critical processes and systems of the Branch are tested twice a year at the above disaster recovery site.

Covid-19 has put to test our robust Business Continuity Plans which include enabling the our staff to work remotely, where possible and the Branch was able to maintain uninterrupted services throughout the pandemic, whilst ensuring the health and safety of our clients and employees.

Role of Insurance

The Branch avails insurance coverage as an external mitigant for 'low probability – high impact' and uncontrollable operational events, which are insurable. Accordingly, insurance coverage has been obtained to cover risks such as cash holdings, cash-in-transit, combined crime/civil liability, directors' and officers' liability, personal accident, public and product liability, damage to property, business interruption and destruction from terrorism.

Outsourcing

The Branch has comprehensive guidelines on outsourcing, which is a combination of local regulations and SCB Group policy and procedures on third party risk management. Governance over outsourcing arrangements is under the oversight of a specialized unit.

Supplier due diligence is carried out both prior to and during the operation of the outsourcing arrangement to ensure any risks are identified and effectively managed. Roles and responsibilities are clearly defined during this process.

The Branch together with relevant Group entities perform appropriate business, operational and technical evaluations and analyses to ensure viability of external outsourcing arrangements. External outsourcing is designed to ensure that the supplier has adequate service delivery capabilities to deliver the agreed service levels, whilst responsibility and control of the outsourced activities remains fully with SCB Branch. A business case document is produced as a result of these evaluations. An inventory of all outsourced activities is maintained and monitored by the Branch through a Group mandated system.

Details of outsourced activities are reported to the Central Bank of Sri Lanka, via the annual calendar plan.

Procurement Management

The Branch is guided by the Procurement Policy issued by Group in order to guide the businesses before on-boarding vendors/service providers for procurement.

43.7 Information and cyber security risk

Information and Cyber Security (ICS) risk is the risk of a breach of confidentiality, integrity and availability (CIA) of SCB Group Information Assets, Information Systems and Technology Infrastructure through cyber attacks, insider activity, error or control failure, which may lead to adverse customer and reputational impact, regulatory censure, financial loss, litigation and the potential for the Group to fail, affecting financial markets and the wider economy.

Impacts of ICS risks could manifest in the form of:

a) **Asset Management** - The risk of not identifying critical information assets will compromise digital resiliency which is the identification and protection of the organization's digital crown jewels. i.e. data, systems, and software applications that are essential to operations.
b) **Awareness and Training** - The risk of Group employees and non-employees/third parties not having adequate security awareness and training may expose the Bank's information assets to loss of CIA. The risk of security staff not having the appropriate skill sets to perform their roles and in line with recent threats and country regulatory requirements.
c) **Identify and Access Management** - The risk of access not being authorized and authenticated will result in Information disclosure, inaccurate or incomplete Information or disruption to business services due to unauthorized access. Close control of user access reduces the risk of external and internal data breaches (due to inappropriate access) leading to financial loss or reputational impact.
d) **Incident Management** - The risk of not having an effective incident management model can impede the Bank's ability to respond and recover from a security incident leading to reputational, regulatory and financial impacts.
e) **Information Protection** - The risk of not protecting SC Group Data, which is transferred electronically or physically. (i.e. data in transit, may lead to reputational loss and loss of confidentiality). In addition, not protecting data at rest may lead to potential loss of integrity.
f) **System Lifecycle Security (including Vulnerability Management)** - Systems, applications and technical infrastructure must be acquired/developed, tested, implemented and maintained in a secure manner to prevent any compromise that could expose the Bank's information assets and systems. The risk of not identifying critical vulnerabilities and remediating through timely patching, code updates or implementation of configuration setting changes may lead to potential loss of CIA.
g) **Secure Configuration Management (including Malware Protection)** - The risk of not securing the Bank's configuration may lead to deviations from our security baseline and changes could result in compromise of CIA, leading in financial loss or reputational impact.
h) **Third Party Management** - The risk of an information security breach arising from Third Parties that process, store, or maintain the Group's Information Assets, Information Systems or Technology Infrastructure.
i) **Network Security** - The risk of inadequate network security may lead to lack of protection to the underlying networking infrastructure and lead to unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure. This may result in a loss of

CIA of information assets.

j) **Secure Logging and Monitoring** - The risk of ineffective logging and monitoring can result in failure to detect unauthorised intrusions and changes, which can weaken our defences and lead to loss of CIA. This may result in financial loss or reputational impact.

Roles and responsibilities

The Group's Information and Cyber Security Risk Type Framework (ICS RTF) defines the roles and responsibilities of the first and second lines of defence in managing and governing ICS Risk respectively across the Group with emphasis on business ownership and individual accountability. The Group Chief Operating Officer has overall first line of defence responsibility for ICS Risk and holds accountability for the Group's ICS strategy. The Group Chief Information Security Officer (CISO) leads the development and execution of the ICS strategy. The Group Chief Information Security Risk Officer (CISRO) function within Group Risk, led by the Group CISRO, operates as the second line of defence and sets the strategy and methodology for assessing, scoring and prioritising ICS risks across the Group. This function has overall responsibility for governance, oversight and independent challenge of ICS Risk.

Mitigation

ICS Risk is managed through a structured ICS Risk framework comprising a risk assessment methodology and supporting policy, standards and methodologies which are aligned to industry best practice models.

In 2020, to ensure ICS Risk management principles prioritise the adverse impact of cyber threat and vulnerability information on confidentiality, integrity and availability of information assets and systems across the Group, the ICS RTF was uplifted to include a threat led risk assessment methodology.

The Group CISRO function monitors compliance to the ICS framework through the review of the ICS risk assessments conducted by Group CISO. All key ICS risks, breaches and weaknesses are reviewed and approved by Group CISRO prior to the execution of mitigating actions. The Group CISO function performs ICS Risk assessment to determine the ICS Risk posture across the Group with reporting to key Group governance committees. Key ICS risks, breaches or weaknesses identified are documented, reviewed and approved by Group CISRO with mitigation activities monitored for completion with statuses reported to the relevant Group governance committees.

BAU Management of ICS Risks

The Banks ongoing efforts to Protect, Enable, Respond, and Engage with information and cyber related issues is benchmarked against industry best practices outlined in the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) ISO 27001 and PCI-DSS.

43.8 Compliance Risk

The Group defines Compliance Risk as potential for penalties or loss to the Group or for an adverse impact to our clients, stakeholders or to the integrity to markets we operate in, through a failure on our part to comply with laws or regulations.

The Group has no appetite for breaches in laws and regulations; while recognising that regulatory non-compliance cannot be entirely avoided, the Group strives to reduce this to an absolute minimum.

Roles and responsibilities

The Group Head, Conduct, Financial Crime and Compliance (CFCC), as Risk Framework Owner for Compliance Risk provides support to senior management on regulatory and compliance matters by:

a) Providing interpretation and advice on regulatory requirements and their impact on the Group;
b) Setting enterprise-wide standards for compliance, through the establishment and maintenance of a risk-based compliance framework, the Compliance Risk Type Framework (Compliance RTF);
c) Setting a programme for monitoring Compliance Risk

The Compliance RTF sets out the roles and responsibilities in respect of Compliance Risk for the Group. All activities that the Group engages in, must be designed to comply with the applicable laws and regulations in the countries in which we operate. The CFCC function is the second line of defence that ensures the overall operation of the framework and for significant areas of laws and regulations, provides oversight and challenge of the first line risk management activities that relate to Compliance Risk.

The Compliance RTF defines Compliance Risk sub-types and, where relevant, assigns responsibility for these to the most appropriate other Principal Risk Type Owner or control function. This ensures that effective oversight and challenge of the first line can be provided by the appropriate second line function. Each of these assigned second line functions sets policies for the organization to comply with, and provides guidance, oversight, and challenge over the activities of the Bank. They ensure that key risk decisions are only taken by individuals with the requisite skills, judgement, and perspective to ensure that the Group's Compliance Risk is appropriately managed.

Mitigation

The Compliance RTF sets the Group's overall approach to the management of Compliance Risk. In support of this, the Compliance function develops and deploys relevant policies and standards setting out requirements and controls for adherence by the Group to ensure continued compliance with applicable laws and regulations.

Through a combination of risk assessment, control standard setting, control monitoring and compliance review activities, the Compliance Risk Framework Owner seeks to ensure that all policies are operating as expected to mitigate the risk that they cover. The installation of appropriate processes and controls is the primary tool for the mitigation of Compliance Risk. In this, the requirements of the Operational Risk Type Framework are followed to ensure a consistent approach to the management of processes and controls.

43.9 Financial crime risk

The Group defines financial crime risk as the 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 Sanctions, Anti-Money Laundering, Anti-Bribery and Corruption and Fraud.

The Group has no appetite for breaches in laws and regulations related to Financial Crime, recognizing that whilst incidents are unwanted, they cannot be entirely avoided.

Roles and responsibilities

The Global Head, Conduct, Financial Crime & Compliance ("CFCC") is the Group's Money Laundering Reporting Officer ("Group MLRO"). The Group MLRO is accountable for oversight of the Group's compliance with its obligations relating to systems and controls for combating money laundering, in accordance with the requirements set out by the FCA in their "Systems and Controls" Handbook.

The Global Head, CFCC is the Risk Framework Owner ("RFO") for Financial Crime as a Principal Risk Type ("PRT") and has delegated all authorities (with exception listed in the Financial Crime Risk Type Framework) to effectively implement this framework to the Co-Heads, Financial Crime Compliance.

As the first line, the business unit process owners have responsibility for the application of policy controls and the identification and measurement of risks relating to financial crime. Business units must communicate risks and any policy non-compliance to the second line for review and approval following the model for delegation of authority.

Locally, financial crime risk is overseen by the Director, Financial Crime Compliance and Country Money Laundering Compliance Officer (CMLCO), in the country CFCC function.

Mitigation

There are three Group policies in support of mitigating financial crime risk:

a) Group Anti-Bribery and Corruption Policy
b) Group Anti-Money Laundering and Terrorist Financing Policy
c) Group Sanctions Policy

These policies are approved by the Co-Heads, Financial Crime Compliance.

The Group operates risk-based controls in support of its financial crime prevention program, including (but not limited to:

a) Client Due Diligence, to meet "Know Your Customer" requirements
b) Surveillance, including Transaction Screening, Name Screening and Transaction Monitoring
c) Global Risk Assessment, to understand and quantify the Inherent and Residual Financial Crime risk across the organization

The strength of these controls is tested and assessed through the Group's Operational Risk Framework, in addition to oversight by the Financial Crime Compliance Assurance and Group Internal Audit functions.

43. 10 Reputational and Sustainability Risk

Reputational risk is the potential for damage to the Group's franchise, resulting in loss of earnings or adverse impact on market capitalisation as a result of stakeholders taking a negative view of the organisation, its actions or inactions – leading stakeholders to change their behaviour.

Roles and responsibilities

The Global Head, Enterprise Risk Management is the Risk Framework Owner for Reputational Risk under the Group's Enterprise Risk Management Framework. For primary risks, the responsibility of Reputational Risk management at country level is delegated to Country Chief Risk Officers. Both the Global Head, Enterprise Risk Management and Country Chief Risk Officers constitute the second line of defence, overseeing and challenging the first line which resides with the Chief Executive Officers, Business Heads and Product Heads in respect of risk management activities of reputational-related risks. The Group recognises that there is also the potential for consequential Reputational Risk should it fail to control other principal risks. Such secondary Reputational Risks are managed by the Risk Framework Owners of each principal risk who are responsible for enhancing existing risk management frameworks to incorporate Reputational Risk management approaches.

Mitigation

The Group's Reputational Risk policy sets out the principal sources of Reputational Risk and the responsibilities and procedures for identifying, assessing and escalating primary and secondary Reputational Risks. The policy also defines the control and oversight standards to effectively manage Reputational Risk. The Group takes a structured approach to the assessment of risks associated with how individual client, transaction, product and strategic coverage decisions may affect perceptions of the organisation and its activities, including, but not limited to, explicit principles related to environment and social risks and defence and dual use goods. Wherever a potential for stakeholder concerns is identified, issues are subject to prior approval by a management authority commensurate with the materiality of matters being considered. Such authorities may accept or decline the risk or impose conditions upon proposals, to protect the Group's reputation. Secondary Reputational Risk mitigation derives from the effective management of other principal risks.

Governance committee oversight

The Brand, Values and Conduct Committee retains Board-level oversight responsibility for Reputational Risk. Oversight from an operational perspective falls under the remit of the Group Risk Committee and the Board Risk Committee. The Group Reputational Risk Committee ensures the effective management of primary Reputational Risk across the Group. The Group Reputational Risk Committee's remit is to:

- Challenge, constrain and, if required, stop business activities where risks are not aligned with the Group's Risk Appetite
- Make decisions on Reputational Risk matters assessed as high or very high based on the Group's primary Reputational Risk materiality assessment matrix, and matters escalated from the regions or client businesses
- Provide oversight of material Reputational Risk and/or thematic issues arising from the potential failure of other risk types

The Group Non-Financial Risk Committee has oversight of the effective management of secondary Reputational Risk. At country level, the Country Chief Risk Officer is the Risk Framework Owner (RFO) of reputational risk, who with the support of the Country Management Team, must actively:

- Promote awareness and application of our policies and procedures regarding reputational risk
- Encourage business and functions to take account of our reputation in all decision-making, including dealings with customers and suppliers
- Implement effective in-country reporting systems to ensure they are aware of all potential issues in tandem with respective business committees
- Promote effective, proactive stakeholder management through ongoing engagement

Reputational risk could arise from the failure of the Group to effectively mitigate the risks in its businesses, including one or more of country, credit, liquidity, market, regulatory, legal, strategic or other operational risk. Damage to the Group's reputation could cause existing clients to reduce or cease to do business with the Group and prospective clients to be reluctant to do business with the Group. All employees are responsible for day-to-day identification and management of reputational risk. These responsibilities form part of the Code and are further embedded through values-based performance assessments.

Risk owners must identify material reputational risks arising from any business activity or transaction that they control and ensure that these are escalated and controlled in accordance with the Group's Reputational Risk Policy and applicable procedures.

Our reputational risk framework covers two areas. Reputational risk management refers to proactively avoiding or mitigating the potential damage that might result from a future reputational risk event (ex ante). Reputational issues management and crisis communication refers to measures to limit damage from a reputational risk event that has already occurred (ex post).

Reputational risk may also arise from a failure to comply with environmental and social standards in our relationship with clients and in our financing decisions. Environmental risk is the potential for material harm or degradation to the natural environment, while social risk is the potential to cause material harm to individuals or communities. Environmental and social risks associated with clients are a key area of risk for the Group and we have continued to develop and enhance our approach to managing such risks over the years.

Reflecting the differing regulatory and legislative frameworks applicable to clients in the Group's markets, we have global sector-specific environmental and social (E&S) standards as set out in our 17 sectoral and three thematic position statements.

We apply these in the provision of financial services to clients who operate in sectors presenting specific risks, and for key issues. These are underpinned by the Equator Principles and the IFC Performance Standards.

The Brand, Values and Conduct Committee retains Board-level oversight responsibility for Reputational Risk. Oversight from an operational perspective falls under the remit of the Group Risk Committee and the Board Risk Committee. The Group Reputational Risk Committee ensures the effective management of primary Reputational Risk across the Group.

The Group Reputational Risk Committee's remit is to:

- Challenge, constrain and, if required, stop business activities where risks are not aligned with the Group's Risk Appetite

- Make decisions on Reputational Risk matters assessed as high or very high based on the Group's primary Reputational Risk materiality assessment matrix, and matters escalated from the regions or client businesses
- Provide oversight of material Reputational Risk and/or thematic issues arising from the potential failure of other risk types.

The Group Non-Financial Risk Committee has oversight of the effective management of secondary Reputational Risk.

43. 11 Model Risk

The Group defines Model Risk as potential loss that may occur as a consequence 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.

Roles and responsibilities
The Global Head, Enterprise Risk Management is the Risk Framework Owner for Model Risk under the Group's Enterprise Risk Management Framework. Responsibility for the oversight and implementation of the Model Risk Type Framework is delegated to the Global Head, Model Risk Management.

The Model Risk Type Framework sets out clear accountability and roles for Model Risk management through the three lines of defence. First-line ownership of Model Risk resides with Model Sponsors, who are the business or function heads and assign a Model Owner for each model. Model Owners represent model users and are responsible for end-to-end model development, ensuring model performance through regular model monitoring and communicating model limitations, assumptions and risks. Model Owners also coordinate the submission of models for validation and approval and ensure appropriate model implementation and use. Second-line oversight is provided by Model Risk Management, which is comprised of Group Model Validation and Model Risk Policy and Governance.

Group Model Validation independently review and grade models, in line with design objectives, business uses and compliance requirements, and highlight identified model risks. Model Risk Policy and Governance team provide oversight of Model Risk, performing regular Model Risk Assessment and risk profile reporting to senior management.

Mitigation
The Model Risk policy and standards define requirements for model development and validation activities, including regular model performance monitoring. Any model issues or deficiencies identified through the validation process are mitigated through the application of model overlays and/or a model redevelopment plan, which undergo robust review, challenge and approval. Operational controls govern all Model Risk-related processes, with regular risk assessments performed to assess appropriateness and effectiveness of those controls, in line with the Operational Risk Type Framework, with remediation plans implemented where necessary.

Governance committee oversight
At the Board level, the Board Risk Committee exercises oversight of Model Risk within the Group. At the executive level, the Group Risk Committee has appointed the Model Risk Committee to ensure effective measurement and management of Model Risk. Sub-committees such as the Credit Model Assessment Committee and Traded Risk Model Assessment Committee oversee their respective in-scope models and escalate material model risks to the Model Risk Committee. In parallel, business and function-level risk committees provide governance oversight of the models used in their respective processes.

Monitoring
The Group monitors Model Risk via a set of Risk Appetite metrics that are approved by the Board. Adherence to Model Risk Appetite and any threshold breaches are reported regularly to the Board Risk Committee and Model Risk Committee.

Models undergo regular monitoring based on their level of perceived Model Risk, with monitoring results and breaches presented to Model Risk Management and delegated model approvers.

Model Risk Management produces Model Risk reports covering the model landscape, which include performance metrics, identified issues and remediation plans. These are presented for discussion at the Model Risk governance committees on a regular basis.

Stress testing

Models play an integral role in the Group's stress testing and are rigorously validated to ensure that they are fit-for-purpose for use under stressed market conditions. Compliance with Model Risk management requirements and regulatory guidelines are also assessed as part of each stress test, with any identified gaps mitigated through model overlays and defined remediation plans.