Risk Management

At OCBC, managing risks is essential for our long-term success and sustainability. We aim to manage risks in a way that protects our operations, while promoting sustainable business growth and delivering value to our customers, shareholders, employees, and communities.

Our risk management approach

The Group has a comprehensive and disciplined risk management approach that covers all types of risks, supported by a strong corporate culture that prioritises accountability, ownership and high ethical standards. The approach involves understanding the sources of risks and their drivers, establishing risk appetites and tolerances to take such risks against business goals and potential impact under adverse circumstances, comprehensive metrics to measure and monitor risk positions on a standalone and aggregated basis, early problem identification and mitigation, reporting and adjustments to risk strategies against cyclical and structural changes.

Risk frameworks are established that cover the required governance and roles and responsibilities and well-documented policies and procedures in taking and managing risks. Given that risks are increasingly interconnected, we assess them holistically. There are established cross-functional assessments of emerging risks that utilise a suite of stress testing and scenario analyses that inform us about the impact of plausible risk factors on our earnings, capital, liquidity, customer segments and obligations. These shape our risk strategies and contingency plans.

Underpinning our risk approach and frameworks are continuous investment in human resources and technology, so as to ensure that the right skills and competencies and data, systems and infrastructure are used in managing risks. The Group is increasingly leveraging on AI technologies to enhance operational efficiency, analytics, decision-making, product innovation and customer engagement. As we adopt AI more widely, we also recognise that there are associated risks in its adoption such as data privacy, data loss, hallucinations, and biases. We are enhancing our risk governance to address such risks comprehensively to ensure that AI is used responsibly.

Risk ownership is a collective responsibility shared between the business and risk functions as elaborated in the Risk Governance and Organisation section.

Risks are generally categorised into five main types, each managed with the necessary skills, resources, systems, policies and procedures. Our risk teams focus on identifying, measuring, sanctioning, monitoring, and reporting risks, while also setting limits and triggers so that the risks and underlying processes are regularly reviewed and approved at the right authority levels. Our frameworks are regularly updated to incorporate best practices and comply with regulatory standards in all the regions where we operate.

Principal risk types

We categorise our risks into five main types:

Table 1: Principal Risk Types

Principal Risks	Definition
Credit Risk	The risk of financial loss due to a borrower failing to meet their financial/contractual obligations.
Market Risk	The risk of financial loss due to fluctuations in market factors such as interest rates, foreign exchange rates and commodity prices.
Liquidity Risk	The risk of not being able to meet financial and cash outflow obligations as they come due.
Operational Risk	The risk of loss from failures in processes, systems, or external events, including money laundering, legal and reputational risks.
Information Security and Digital Risk	The risk of compromising confidentiality or integrity of information, cyber threats and technology failures.

For more details on how we manage these risks, please refer to the specific sections in our report.

Risk Management

Environmental, social and governance (ESG) and climate risks

Managing ESG and climate risks is vital to our operations, as they affect our credit, market, liquidity, operational, and reputational risks. We take an integrated approach to assessing and managing these "cross-cutting" risks, which is part of our overall risk framework. Our practices include monitoring ESG metrics, conducting climate scenario analyses, and ensuring that customers in high-risk sectors undergo thorough assessments in managing their ESG, transition and physical risks. Time-bound action plans or covenants may be imposed on customers and transactions posing significant reputational risks are escalated to the Reputational Risk Review Group for further review and clearance.

We are committed to integrating quantitative ESG and climate risk metrics into our practices while enhancing climate scenario analysis methodologies. Our approach is guided by industry developments, data availability, and ongoing dialogue with regulators. For more details on our initiatives, please refer to our Sustainability Report 2024 on Climate Action and Responsible Financing.

Risk Governance and Organisation

A robust risk governance structure ensures that we have effective oversight and accountability of risk. Our Board of Directors have ultimate responsibility for the effective management of risk. The Board establishes the corporate strategy and approves the risk appetite within which senior management executes the strategy. The Group's risk governance and oversight structure, which banking subsidiaries and Great Eastern Holdings (GEH) are aligned with, is shown on page 79.

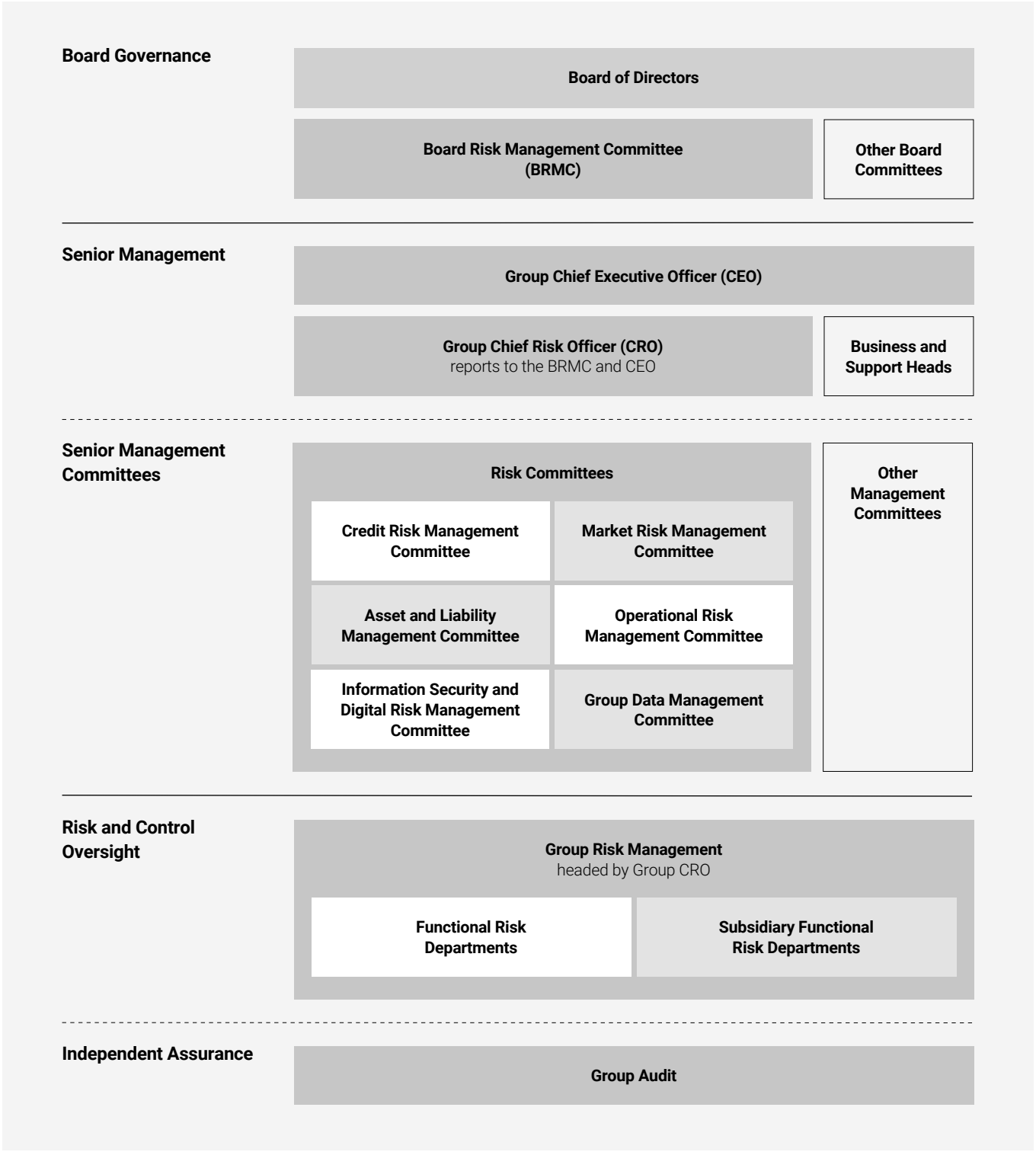
The Board Risk Management Committee (BRMC) is the designated board committee that oversees risk management matters. It ensures that the Group's overall risk management philosophy and principles and risk appetite are aligned with the corporate strategy. The BRMC has oversight of credit, market, liquidity, information security and digital, operational, conduct, money laundering and terrorism financing, fraud, legal, regulatory, strategic, ESG and fiduciary risks, as well as any other category of risk that may be delegated by the Board or deemed necessary by the BRMC.

The BRMC provides quantitative and qualitative guidance to major business units and risk functions to guide risk-taking. BRMC and senior management regularly review our risk drivers, risk profiles, risk management frameworks and policies, and compliance matters. Please refer to the Corporate Governance Chapter for more information on the BRMC.

Dedicated functional risk committees comprising senior management from risk taking and risk control functions have been established to facilitate close risk oversight. These committees are supported by the functional risk management units under the Group Risk Management Division (GRM).

GRM is headed by the Group Chief Risk Officer (CRO). The Group CRO is a member of the Group Management Executive Committee and functional risk committees. GRM's day-to-day responsibilities involve providing independent risk control and managing credit, market, liquidity, information security and digital, operational and ESG risks. It provides regular risk reports and updates on developments in material risk drivers and potential vulnerabilities, and recommends mitigating actions to senior management, risk committees, the BRMC and the Board. At the Group level, GRM also provides functional oversight to the banking subsidiaries and GEH.

GEH and OCBC Indonesia are listed companies. Their annual reports contain information on their risk management frameworks and practices. Their risk management frameworks, policies and practices are appropriately aligned with the Group's risk standards.


Board Governance
Board of Directors
Board Risk Management Committee (BRMC)
Other Board Committees
Senior Management
Group Chief Executive Officer (CEO)
Group Chief Risk Officer (CRO)
reports to the BRMC and CEO
Business and Support Heads
Senior Management Committees
Risk Committees
Credit Risk Management Committee
Market Risk Management Committee
Asset and Liability Management Committee
Operational Risk Management Committee
Information Security and Digital Risk Management Committee
Group Data Management Committee
Other Management Committees
Risk and Control Oversight
Group Risk Management
headed by Group CRO
Functional Risk Departments
Subsidiary Functional Risk Departments
Independent Assurance
Group Audit

Risk Management

Three lines of defence

All employees are responsible for identifying and managing risk, a responsibility embedded in our corporate culture and robust internal control environment. This is operationalised via a three-line structure that distinctly outlines the roles, responsibilities and accountability of risk.

Table 2: Three Lines of Defence

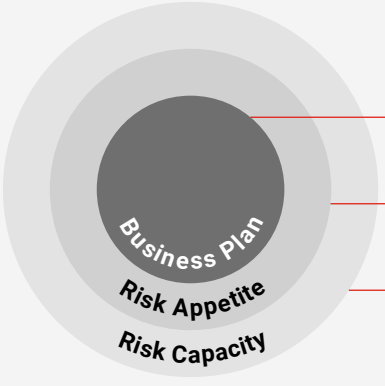
First Line	Second Line	Third Line
Day-to-day Risk Management	**Risk and Control Oversight**	**Independent Assurance**
Business and Support Units: • Owns and manages risks arising from their business activities on a day-to-day basis. • Carries out business activities that are consistent with the Group's strategy and risk appetite. • Operates within the approved boundaries of our policies and limits and complies with applicable laws and regulations.	**Risk and Control Function:** • Independently and objectively identifies and assesses the risk-taking activities of the first line. • Establishes relevant risk management frameworks, policies, processes and systems. • Provides independent identification, assessment, monitoring and reporting of the Group's risk profiles, portfolio concentrations and material risk issues.	**Group Audit:** • Independently provides assurance to the Group CEO, Audit Committee and Board on the adequacy and effectiveness of our risk management and internal control systems. • Evaluates the overall risk awareness and control consciousness of management in discharging its supervisory and oversight responsibilities.

Risk Appetite

Our aim is to manage risks in a prudent and sustainable manner for the long-term viability of the Group. The Board determines the Group's risk appetite, defining the level and nature of risks that we can undertake on behalf of our shareholders while maintaining our commitments to customers, regulators, employees and other stakeholders. Business plans take into account the corporate strategy, the forward-looking operating environment and potential risks assessed against our risk appetite. Our risk appetite is operationalised across the Group through our policies, processes and limits to manage both financial and non-financial risks. Together, these components form our Risk Appetite Framework, which articulates our risk appetite at the Group level and guides operations within our major business units.

Specific risk tolerance levels are defined for different portfolios based on our corporate strategy and the inherent risk characteristics of each portfolio. We closely monitor performance against these risk tolerances and report findings in relevant forums.

Senior business and risk managers participate in regular forums to review macroeconomic and financial developments and discuss operating conditions, event risks and potential 'dark clouds' that may significantly impact our earnings or solvency. These risks are measured via stress tests as well as segment-specific and ad hoc event-specific portfolio reviews. The results are used to assess the potential impact of various scenarios on our earnings and capital, and to identify vulnerabilities of material portfolios and trigger appropriate risk management actions.



Business Plan	Demand for Risk and Financial Resources to meet our business objectives
Risk Appetite	Level and nature of risk deemed acceptable while ensuring a sufficient buffer in the Risk and Financial Resources
Risk Capacity	Supply of Risk and Financial Resources such as Funding and Capital

We conduct an annual Internal Capital Adequacy Assessment Process (ICAAP) that incorporates the results of stress tests for various risk types. The aim is to assess whether we are capable of maintaining sufficient capital levels under a forward-looking operating environment and in severe stress scenarios. Appropriate risk-mitigating actions are taken to manage potential risks.

Credit Risk Management

Credit risk arises from our lending activities to retail, corporate and institutional customers. It also includes counterparty and issuer credit risks arising from our underwriting, trading and investment banking activities.

Credit risk management approach

Our credit risk management framework offers a proactive strategy for overseeing credit risk across the Group's lending operations, establishing clear objectives and minimum standards. Our approach to managing credit risk is thorough and multi-faceted, ensuring we effectively mitigate potential losses while supporting our lending and underwriting activities. The framework establishes credit approval authorities, concentration limits, risk-rating methodologies, portfolio review parameters and guidelines for management of distressed exposures.

It leverages the expertise and judgment of credit specialists, ensuring effective risk management tailored to the distinct characteristics of different portfolios and customer segments. All credit exposures must be approved by credit approving officers with the level of credit authority delegated to officers based on their experience, seniority and track record. Specific policies and procedures are implemented for major customer segments as shown in Table 3.

Table 3: Credit Risk Management Approach for Major Customer Segments

Consumers and Small Businesses	• Evaluate credits based on established product programs acquisition strategies, and specific customer selection criteria, while employing advanced models for consistent credit decisions and due diligence. Deviations from the credit criteria are approved by dedicated credit approving officers. • Monitor portfolio credit risk using comprehensive MIS, behavioural models, and stress testing to proactively identify potential weak credits.
Corporate and Institutional Customers	• Perform individual credit assessments through independent evaluations by experienced officers, adhering to target market and risk acceptance criteria, and base decisions on detailed qualitative and quantitative analyses including rating models. • Ensure joint credit approvals between business and credit risk units for objectivity, while conducting regular reviews and stress tests to monitor credit quality and identify potential weaknesses early.
Private Banking Customers	• Carry out independent assessments of individual credits by experienced officers, following predefined risk acceptance criteria and collateral requirements. • Ensure joint credit approvals between business and credit risk units for objectivity, while regularly monitoring credit conduct and conducting stress tests to identify potential issues early.

Counterparty credit risk management

Counterparty credit risk arises from the potential default of a counterparty during our trading and/or banking activities including in derivatives and debt securities. The credit exposure to a counterparty is measured as the sum of current mark-to-market value of the transactions plus an appropriate add-on for potential future exposures due to market price fluctuations. This risk also covers settlement risk, which is the potential loss incurred if a counterparty fails to fulfil its obligation after the Bank has performed its obligation under a contract or agreement at the settlement date.

We have a dedicated risk management team to manage counterparty credit risk. The team assesses risk at the individual counterparty level, country and sector portfolio level, and product level following a set of policies and procedures. Each counterparty undergoes robust credit assessment, including the suitability of the product offered. Credit risk mitigation tools are used as needed to manage counterparty credit risk. Please refer to the Credit Risk Mitigation on page 82 for details.

We independently manage our credit exposures through daily limit monitoring, escalation of excesses, pre-deal excess approvals, regular risk reporting and stress testing. In addition, we have an established policy and process to identify, manage and report wrong-way risk, which arises when the quantum of exposure to a counterparty increases as the counterparty's credit quality deteriorates.

Risk Management

Credit risk mitigation

Credit risk mitigation is managed via various measures such as holding collateral, buying credit protection and setting netting arrangements to reduce credit risk exposures. Risk mitigation does not replace our proper assessment of the obligor's ability to repay, which remains the primary source of repayment. Our credit policies outline the key considerations for eligible credit risk mitigants including legal certainty and enforceability, correlation, liquidity, marketability, counterparty risk of the credit protection provider and collateral-specific minimum operational requirements. Eligible physical and financial collateral includes cash, real estate, marketable securities, standby letters of credit and credit insurance.

Where collateral is taken, appropriate haircuts are made to the value to reflect its inherent nature, quality, liquidity and volatility. Regular independent valuations of the collateral are conducted. We also monitor our collateral holdings to maintain diversification across asset classes and markets. We accept guarantees from individuals, corporates and institutions as a form of support. Where guarantees are recognised as credit risk mitigants via the probability of default (PD) substitution approach, we have established eligibility criteria and guidelines.

Netting, collateral arrangements, early termination options and central clearing mechanisms are common risk mitigation tools to manage counterparty credit risk. In approved netting jurisdictions, netting agreements allow us to offset our obligations against what is due from the counterparty in the event of a default, thereby reducing credit risk exposure.

Collateral arrangements are typically governed by market standard documentation such as the International Swaps and Derivatives Association (ISDA) and Credit Support Annexes (CSA) or Global Master Repurchase Agreements (GMRA). Such arrangements require the posting of additional collateral if the mark-to-market exposures exceed the agreed threshold amount. We apply a haircut to the value of the eligible collateral to cover potential adverse market volatility. Regulatory margin requirements may apply to the agreed threshold amount. ISDA agreements may also include rating triggers to allow for transaction termination or require additional collateral if a rating downgrade occurs.

Given our current investment grade rating, a one-notch rating downgrade would result in a minimal increase in collateral to be posted. Where possible, we also clear Over-the-Counter (OTC) derivatives transactions through approved central clearing counterparties, thereby replacing the counterparty's credit risk with that of a highly regulated and better credit rated central clearing counterparty.

Credit portfolio management

Credit portfolio management focuses on managing the collective or aggregate risk of our credit portfolios, instead of the credit risk of individual borrowers. We have developed and implemented a range of capabilities to identify, measure and monitor credit risk at the portfolio level. These capabilities include:

- **Portfolio segmentation**
  This is the process of grouping credit exposures that are similar in nature. It involves using attributes that represent common business drivers, such as geography, industry and business segment, as well as common risk drivers such as exposure to material downside risks like a property price correction, a sharp hike in interest rates, or a country risk event.

- **Portfolio modelling**
  This includes using internal rating models to quantify the exposure risk, default risk and potential losses of our borrowers. Please refer to Table 4 for information on our internal rating models. We also use stress test models to simulate the potential increase in our credit losses and Credit Risk Weighted Assets (CRWA) under stressed scenarios.

  Overview of internal rating models
  Internal credit rating models and their components such as PD, loss given default (LGD) and exposure at default (EAD) are used in limit setting, credit approval, portfolio monitoring and reporting, remedial management, stress testing and assessment of capital adequacy and portfolio allowances.

  Our model risk management framework governs the development, validation, application and maintenance of rating models. Models are developed with the active participation of credit experts from risk taking and risk control units. They are subject to independent validation before implementation, followed by annual reviews to ensure that performance standards (which take into consideration regulatory requirements and industry best practices) are continually met. In addition, Group Audit annually reviews the robustness of the rating process and the effectiveness of the independent validation process. Approval for the adoption and continued use of material models rests with the BRMC. In addition, models that are used in regulatory capital assessment must be approved by the regulators.

  While our internal risk grades are not explicitly mapped to external credit ratings, they may correlate with external credit ratings in terms of the PD ranges because the factors used to rate obligors are similar. As such, an obligor rated poorly by an external credit rating agency is likely to have a weak internal risk rating as well.

  IRB models and portfolios
  Table 4 describes the approaches used to estimate the key parameters for Advanced Internal Ratings-Based (A-IRB) and Foundation Internal Ratings-Based (F-IRB) credit risk models used to calculate CRWA.

Table 4: Key Components of Internal Ratings-Based (IRB) Models

IRB Models and Portfolios	PD	LGD and EAD
A-IRB approach covers major retail portfolios such as residential mortgages, credit cards, auto loans, insurance financing, small businesses and margin lending	• PD is estimated based on the application and behaviour scores of obligors. • PD models are calibrated to reflect the expected long-run average one-year default rate over an economic cycle.	• Product, collateral and geographical characteristics are major factors. • LGD models are calibrated to reflect the economic loss under downturn conditions. • EAD models are calibrated to reflect the default-weighted average and economic downturn conditions.
F-IRB (Non-Supervisory Slotting) approach covers major wholesale portfolios such as sovereigns, banks, non-bank financial institutions, corporate real estate (including income producing real estate) and general corporates	• PD models are statistical based or expert judgement models that use both quantitative and qualitative factors to assess an obligor's repayment capacity and are calibrated to reflect the expected long-run average one-year default rate over an economic cycle. • Expert judgement models based on inputs from internal credit experts are typically used for portfolios with low default rates.	• LGD and EAD are estimated based on rules prescribed in MAS Notice 637.
F-IRB (Supervisory Slotting) approach covers other specialised lending portfolios such as project finance, object finance and commodities finance	• Obligors are mapped to the five supervisory slotting categories prescribed in MAS Notice 637 based on regulatory loan classifications.	• LGD and EAD are estimated based on rules prescribed in MAS Notice 637.

- **Portfolio reporting**
  This includes internal and external reporting of portfolio risk information to the respective stakeholders. These reports provide a better understanding of how the credit portfolio risk trends are evolving in response to the changing operating environment and downside risks. Regular risk reports covering detailed metrics for credit portfolio exposures, quality, concentrations and hotspots covering dimensions such as geography, industry and business segment are provided to Senior Management and the Board for making timely and better-informed decisions.

Using insights from portfolio modelling and reporting, we allocate appropriate risk and financial resources such as funding and capital to support growth opportunities. We use these insights to set credit concentration limits and manage potential risks stemming from adverse changes in the operating environment. The design of these limits considers direct and indirect risk drivers, such as economic sector, industry and geographic location, collateral type or other credit risk mitigation.

We also utilise these insights to identify and quantify more vulnerable segments and take proactive risk management actions where appropriate. This is especially crucial during periods of slow economic growth, high inflation, elevated interest rates, and heightened geopolitical tensions. These actions include actively tracking potentially vulnerable exposures; setting limits on maximum exposure; closely monitoring and reviewing vulnerable exposures; stress testing to assess potential credit impact; implementing risk mitigation and remedial management measures; and ensuring prudent provisioning and adequate capital allocation if needed.

Remedial management

Processes are in place to foster early identification of vulnerable borrowers. The quality of our credit portfolios is proactively monitored and discussed at various risk forums. Action plans to remediate deteriorating trends are worked out and reviewed at such forums.

Risk Management

We classify our credit exposures as restructured assets when we grant non-commercial concessions to borrowers who are unable to meet their original repayment obligations. We further classify a restructured credit exposure into the appropriate non-performing grade based on our assessment of the borrower's financial condition and ability to repay under the restructured terms. Such credit exposure must comply fully with the restructured terms for a reasonable period before it can be restored to performing status in accordance with MAS Notice 612 (Credit Files, Grading and Provisioning).

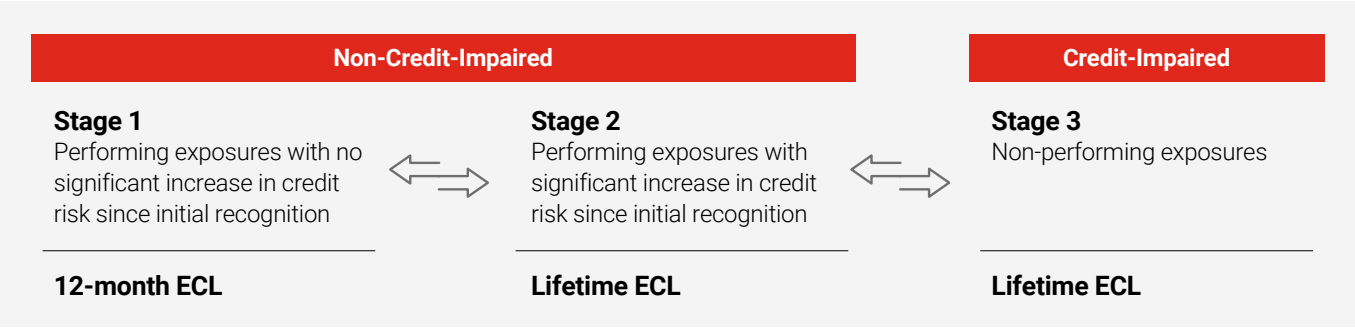
Dedicated remedial management units manage the restructuring, work-out and recovery of non-performing assets (NPAs) for wholesale portfolios. The goal is to rehabilitate NPAs where possible or maximise recoveries for NPAs that are on an exit strategy. For retail portfolios, we develop appropriate risk-based and time-based collections strategies to maximise recoveries while trying to minimise impact to our customers. We use data such as delinquency buckets and adverse status tags for delinquent consumer loans to regularly analyse, refine and prioritise our collection efforts.

Credit loss allowances

We maintain sufficient allowances to absorb credit losses inherent in our loan portfolios. Allowances for Expected Credit Losses (ECL) are recognised for credit-impaired and non-credit-impaired exposures in accordance with Singapore Financial Reporting Standard (International) 9: *Financial Instruments* (SFRS(I) 9) and MAS Notice 612 through a forward-looking ECL model.

We assess our ECL allowances on a forward-looking basis, taking into account the three stages of credit risk below.

Stages of Credit Risk and Expected Credit Losses



Please refer to Notes 2.11 and 2.21 in the Group's Financial Statements for more information on impairment allowances.

Market Risk Management

Market risks arise primarily from our trading, customer servicing and balance sheet management activities. Given the volatile macroeconomic environment, it is paramount that the management of market risk is robust and timely. This is achieved through the market risk management approach, which involves the identification, measurement, monitoring, reporting and control of market risks.

Market risk management approach

Group level market risk policies and procedures are established to provide common guidelines and standards for managing market risks. We regularly review our market risk management strategy and limits, which are established in accordance with our risk appetite and are aligned with our business strategies, taking into account prevailing macroeconomic and market conditions.

Identification

Our internal approval processes ensure that market risk is properly identified and quantified, allowing us to manage and mitigate such risks.

Measurements

- **Value-at-risk**
  Value-at-risk (VaR) is a key metric used to quantify market risk exposures arising from our trading portfolio activities. VaR is measured and monitored by individual market risk components, namely interest rate risk, foreign exchange risk, equity risk, credit spread risk and commodity risk, as well as at the aggregate level. Our VaR model is based on the historical simulation approach, calibrated at the 99% confidence level and a one-day holding period. A 99% confidence level means that, statistically, losses on a single trading day may exceed VaR on average, once every 100 days. Table 5 provides a summary of the Group's trading VaR profile by risk type as of 31 December 2024 and 31 December 2023.

- **Other risk measures**
  As interest rate movements are a key driver of our market risk exposure, Present Value of a Basis Point (PV01), which measures the change in value of interest rate-sensitive exposures resulting from a one basis point increase across the entire yield curve, is an important measure that is monitored on a daily basis. Other than VaR and PV01, we use risk metrics such as notional positions, Profit & Loss (P&L) for One Basis Point Move in Credit Spreads (CS01) and other risk variables for specific exposure types.

Table 5: VaR by Risk Type – Trading Portfolio

	2024				2023			
SGD Million	**End of the period**	**Average**	**Minimum**	**Maximum**	End of the period	Average	Minimum	Maximum
Interest Rate VaR	**6.3**	**6.9**	**4.4**	**10.8**	4.2	7.6	4.2	12.6
Foreign Exchange VaR	**2.8**	**2.3**	**0.8**	**8.0**	2.5	3.1	1.1	9.3
Equity VaR	**3.6**	**2.5**	**0.8**	**4.3**	1.0	1.9	0.8	3.0
Credit Spread VaR	**2.0**	**2.8**	**1.7**	**4.6**	2.2	5.7	1.9	12.0
Commodity VaR	**0.0**	**0.4**	**0.0**	**1.7**	0.0	0.0	0.0	0.2
Diversification Effect[1]	**(9.5)**	**(8.6)**	**NM[2]**	**NM[2]**	(4.4)	(9.1)	NM[2]	NM[2]
Aggregate VaR	**5.2**	**6.3**	**4.1**	**10.6**	5.5	9.2	5.0	16.0

[1] Diversification effect is computed as the difference between Aggregate VaR and the sum of asset class VaRs.
[2] Not meaningful as the minimum and maximum VaRs may have occurred on different days for different asset classes.

Stress testing and scenario analysis

We perform stress testing and scenario analyses to assess and quantify potential losses from unlikely but plausible extreme market conditions. We regularly review and adjust the stress scenarios to ensure their relevance to our trading portfolio activities and risk profile, as well as current and forecasted economic conditions. These analyses determine if potential losses from such extreme market conditions are within our risk tolerance. In addition to regular stress scenarios, we also use ad hoc event-specific stress scenarios to assess the potential impact of specific market conditions on our market risk exposures.

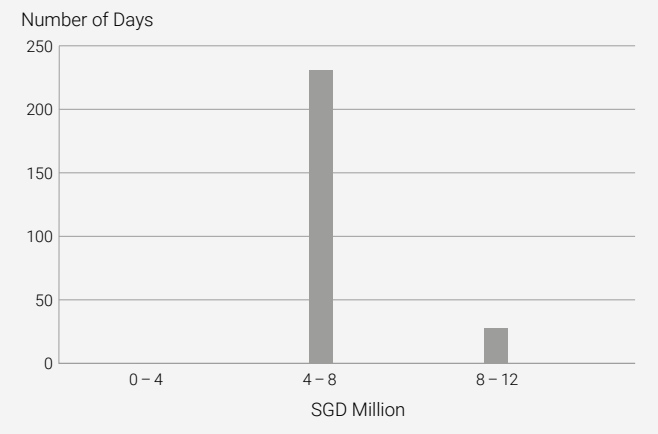
Risk monitoring, reporting and control

- **Limits**
  Trading units may only undertake authorised trading activities for approved products. All trading risk positions are monitored on a daily basis against approved and allocated limits. Trading activities are conducted within approved mandates and are dynamically hedged to remain within limits. Hedge effectiveness is enforced through independent limit monitoring to ensure compliance with market risk limits. Limits are approved to reflect our risk appetite and manage the downside risks from trading opportunities, with clearly defined exception escalation procedures. We report exceptions, including temporary breaches, promptly to Senior Management and the Board. We also manage market risk exposure holistically by using multiple risk limits (VaR and risk sensitivities), P&L stop loss and other measures.

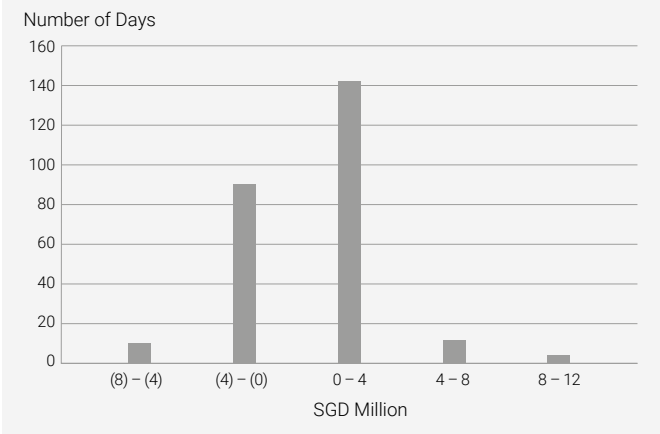
- **Model validation**
  Model validation is an integral part of our risk control process. Financial models are used to price financial instruments and calculate VaR. We ensure that the models used are fit for their intended purposes through periodic independent validation and reviews. To enhance the integrity of the trading P&L and risk measures generated, we source market rates independently for risk measurement and valuation.

- **Back testing**
  To ensure the continued integrity of our VaR models, we back-test the VaR against actual trading P&Ls and hypothetical P&Ls daily to confirm that the models do not underestimate our market risk exposures. The charts below illustrate the Frequency Distribution of Group Trading Book's Daily Total VaR and P&L.

Frequency Distribution of Group Trading Book's Daily Total VaR (One Day Holding Period) for FY 2024



Frequency Distribution of Group Trading Book's Daily Hypothetical P&L for FY 2024



Risk Management

Asset Liability Management

Asset liability management is the strategic management of our balance sheet structure and liquidity requirements. It covers liquidity sourcing and diversification, as well as interest rate and structural foreign exchange management.

Asset Liability Management (ALM) approach

The Group has an established ALM risk framework that oversees and manages the Liquidity, Interest Rate Risk in the Banking Book (IRRBB) and Structural Foreign Exchange (SFX) risk exposures. Group Asset and Liability Committee (ALCO) provides stewardship, and regularly reviews our ALM risk profiles to ensure the management approach is in line with our business strategies and risk appetite, taking into account prevailing macroeconomic and market developments.

Liquidity risk

The objective of liquidity risk management is to ensure that the Group continues to fulfil its financial obligations and can undertake new business, by effectively managing liquidity and funding risks within its risk appetite. Managing liquidity involves addressing funding needs through maintaining adequate and diversified sources of liquidity and balancing cost effectiveness.

- **Identification**
  Liquidity risk arises from cashflow mismatches in maturing assets, liabilities and off-balance sheet items. It is identified by monitoring risk metrics and early warning indicators that signal potential liquidity risks stemming from market developments.

- **Measurements**
  Liquidity risk is measured based on the cash flow mismatches arising from assets, liabilities and off-balance sheet items, projected on both contractual and behavioural bases under business-as-usual conditions and stressed market scenarios. Concentration and regulatory liquidity ratios measure the effective diversification of funding sources and ability to meet stressed liquidity conditions.

- **Risk monitoring, reporting and control**
  Liquidity risk positions are continuously monitored against approved liquidity risk limits and triggers, established in accordance with the Group's risk appetite. A rigorous review, oversight and escalation process facilitates prompt escalation and remediation of any limit exceptions.

- **Stress testing and scenario analysis**
  Stress testing is regularly conducted under a variety of regulatory, historical and market scenarios to assess the potential impact of market events on the Group's liquidity risk profile. The stress testing outcomes are applied to shape effective funding strategies, liquidity policies and contingency funding plans to minimise the impact of any liquidity crunch.

Interest Rate Risk in the Banking Book (IRRBB)

IRRBB refers to the current and prospective risk of interest rates to the Group's capital and earnings. With a broad range of products spanning different interest rate structures, curves and maturities, the repricing profile of assets and liabilities can be mismatched. As interest rates and yield curves move, these mismatches may affect the Group's economic value and potentially lead to a decline in earnings. The primary goal of the management of IRRBB is to ensure that the impact of these events on our interest rate risk exposures are consistent with our risk appetite and maintained within the defined risk tolerance.

- **Identification**
  Interest rate risk varies with repricing periods, currencies, embedded options and interest rate bases. It arises from interest rate sensitive instruments which are:
  - Repricing at different times (gap risk)
  - Referencing different interest rate benchmarks (basis risks)
  - Possessing optionality with respect to timing of cashflows or interest rate reset under different circumstances (optionality risk).

- **Measurements**
  The Group manages IRRBB using both earnings- and capital-based measures.
  - Net Interest Income (NII) sensitivity estimates the potential earnings impact under various interest rate scenarios, assuming the Group's balance sheet remains unchanged over the next one year. Interest rate caps and floors are applied in interest cashflow projections in line with contractual obligations and business practices.
  - Economic Value of Equity (EVE) sensitivity and present value of one basis point (PV01) simulate the potential impact of various interest rate shock scenarios on the Group's capital. They are computed by discounting repricing cashflows, including commercial margins and spreads, using risk-free rates or a proxy for currencies without an active risk-free market rate.

The above measures take into account the impacts of loan prepayment and fixed deposit early redemption, estimated based on statistical analyses of historical customer behaviours, product features and market indicators. For non-maturity deposits which do not have explicit maturity or repricing dates, the repricing profile is determined by studying the elasticity of deposit rates to market interest rates and the volatility of deposit balances. These modelling assumptions are independently validated, reviewed and approved by Group ALCO and consistently applied across public disclosure and internal risk monitoring.

- **Risk monitoring, reporting and control**
  Interest rate risk positions and metrices are computed at least monthly and closely monitored against approved risk limits and triggers. Interest rate derivatives are commonly used as hedging instruments to manage IRRBB within risk limits, with hedge accounting adopted where appropriate.

- **Stress testing**
  Regular stress testing is performed to evaluate whether the Group's capital is sufficient to withstand the impact of extreme interest rate movements on the balance sheet. Such tests are performed across historical, hypothetical and regulatory interest rate shock scenarios as well as internal scenarios, to assess the potential impact of adverse scenarios on the Group's financial condition. These assessments serve as critical inputs for shaping interest rate risk profiles and management strategies.

Structural Foreign Exchange (SFX) risk

SFX exposures arise from non-Singapore Dollar investments in overseas branches, subsidiaries, other strategic investments and property assets. They affect the Group's Capital Adequacy Ratio (CAR) and total equity through the impact on Foreign Currency Translation Reserves (FCTR).

- **Identification**
  The objective of SFX risk management is to protect the capital and financial soundness of the Group by managing the potential impact arising from adverse FX movements, through monitoring, stress testing and hedging where appropriate.

- **Measurements, monitoring, reporting and control, and stress testing**
  We implement a comprehensive risk management methodology to ensure appropriate and effective risk capturing and controls around SFX exposures. We monitor the SFX impact on our capital and CAR stability and perform regular assessments to ensure that potential losses under severe market stress scenarios are within our risk tolerance.

Other risk

Non-structural foreign exchange exposures in our banking book are largely transferred to our trading book for foreign exchange risk management. In addition, we are exposed to credit spread risk through the holding of High-Quality Liquid Assets (HQLA) in our banking book to comply with the Liquidity Coverage Ratio (LCR) requirements. While the default risk for HQLA is low, their value could be sensitive to changes in credit spreads. This risk is monitored against approved CS01 limits on a daily basis and subject to historical and anticipatory stress testing. The other risk residing in our banking book is equity price risk arising from our equity investments in listed and non-listed companies. Equity investments (excluding those held by GEH) form an insignificant portion of our overall securities portfolio.

Operational Risk Management

Operational risk is the risk of loss caused by failures in internal processes, systems, people or external events which is present in all banking products, activities, processes, and systems. It encompasses a range of non-financial risks, including fraud; money laundering, terrorism financing and sanctions risk; third-party risk; physical and personnel security risk; conduct risk; business continuity risk; unauthorised trading risk, regulatory risk as well as legal and reputational risk.

Operational risk management approach

Our operational risk management framework sets out our approach to managing and controlling the operational risks arising from the Group's business activities and operations. The framework is supported by various programmes that ensure preparedness and minimise the impact of any adverse event through timely response, recovery, and adaptability of Critical Business Services and Functions.

Senior Management and the Board receive regular updates on the operational risk profile, which includes operational risk events, key risk indicators, material issues and trends. Additionally, the Board receives an annual assurance report assessing the adequacy and effectiveness of our internal controls and risk management systems.

Strengthening our Operational Resilience

Operational Resilience refers to our ability to minimise the risk of business interruptions caused by operational failures, while ensuring the continued delivery of Critical Business Services and Functions during disruptions. To achieve this, the Group is committed to proactively anticipate and prevent potential operational risk events through robust risk management practices.

Our strategy for Operational Resilience builds on our existing programmes such as business continuity management, crisis management, physical security risk management, third-party risk management, technology risk management and cyber security. The robust risk management practices adopted by these programmes enable us to mitigate disruption risks by anticipating, preparing for, responding to, recovering from, and learning from events.

- **Key components of Operational Resilience**
  Business continuity management
  Business continuity management encompasses strategies and plans that enable organisations to maintain Critical Business Services and Functions to minimise disruption, downtime and safeguard resources. Our comprehensive Business Continuity Management programme identifies these services and functions, along with their Service Recovery Time Objectives. The necessary processes, systems, and resources required for service delivery are mapped out and regularly reviewed to identify key dependencies.

Risk Management

Through thorough Business Impact Analysis, we develop Business Continuity Plans that outline recovery strategies for various disruption scenarios. Annual tests are conducted to ensure the effectiveness of these strategies and to confirm that the target recovery time objectives can be met.

Incident response and crisis management
Incident response and crisis management entail a systematic approach to respond to crisis incidents such as public disorder, crime, terrorism, natural hazards, technology disruptions and cyber-attack, that may disrupt normal operations.

Robust incident response procedures and crisis management processes are established and tested regularly through simulation exercises, drills, and participation in industry level exercises to enhance preparedness and to validate the effectiveness of established processes. Additionally, our Global Incident Monitoring Centre continuously monitors global security incidents that could impact the safety of our employees and the security of our premises, ensuring that timely response measures can be taken as needed.

Physical security risk management
Physical security are measures put in place to safeguard the Group's physical assets, facilities, personnel and customers in our premises from threats.

Our physical security programme provides the foundation for a safe and secured environment for both customers and employees. Regular physical security risk assessments are conducted by in-house and external security experts, alongside continuous monitoring of emerging threats, including those related to climate change. Additionally, periodic physical security penetration exercises are conducted to ensure the vigilance and preparedness of our security personnel.

Third-party risk management
Third-party risk refers to the potential disruption to the Group's operations arising from service failures, breaches of confidential information, or non-compliance with regulatory requirements by the third parties we engage.

To effectively manage these risks, we have established a comprehensive third-party risk management programme. The programme includes a stringent onboarding process for third-party service providers, ongoing monitoring and periodic due diligence assessment. These measures are designed to minimise any potential adverse impact to our operations.

Operational Resilience capabilities also encompass technology risk management, disaster recovery, information security and data recovery controls. Please refer to the Information Security and Digital Risk Management Section for more information.

- **Other key aspects of operational risk management**
  New product review and approval
  Each new product or channel undergoes a stringent review process, to identify and mitigate inherent risks. This ensures prudent allocation of resources and capital, compliance with regulatory requirements, and effective risk management to support sustainable business growth initiatives.

Conduct risk
To promote prudent risk taking and desired risk behaviour among employees, we have in place the Material Risk Takers and the Employee Conduct Triggers programmes. These programmes focus on appropriate incentive structures and regularly reviewed indicators related to various aspects of the employee code of conduct.

Fraud risk
The Group adopts a zero-tolerance stance against fraud, bribery and corruption. All instances of suspected fraud, bribery or corruption events will be treated seriously and dealt with swiftly. In addition to disciplinary actions meted out to employees who engage in fraud misconduct, managers of the function may also be held accountable for the failure of control.

To protect our customers from fraud and scam activities, our fraud surveillance systems are continuously enhanced to adapt to evolving fraud and scam typologies, as well as changes in the regulatory landscape. Our transaction monitoring capabilities enable us to detect and alert customers to suspicious account activities, effectively preventing potentially fraudulent transactions from being completed.

Unauthorised trading risk
Early warnings of issues that could result in Rogue Trading/ Unauthorised Trading (RT/UT) and Markets Conduct Risk are detected through a Global Markets Trade Surveillance programme. The ongoing surveillance and governance drives risk management actions to rectify any control gaps in the end-to-end functions and allow management to have a single view of all controls for RT/UT and Markets Conduct Risks.

Anti-money laundering / countering the financing of terrorism
Robust risk surveillance capabilities that leverage AI and data analytics are in place for dynamic monitoring and detection of suspicious networks, emerging financial crime trends and risk typologies.

Regulatory risk
The Group maintains strong vigilance over developments in the regulatory environment to proactively manage new, emerging, and potential compliance risk exposures. Through our regulatory change management process, we ensure all new regulations and regulatory changes are adequately assessed and timely implemented by the Bank to meet its regulatory obligations.

Insurance management
Financial lines insurance such as Bankers Blanket Bond, Professional Indemnity, Directors and Officers Liability, Cyber and Network Security are in place to cover key non-financial risks.

Information Security and Digital Risk Management

Information security and digital risk is a business risk that comprises the risk domains of information, cyber and technology risks. Effective management of information security and digital risk is key to ensuring the confidentiality, integrity and availability of our information and critical systems. This minimises any material impact to our customers and businesses arising from unforeseen issues or events.

Information security and digital risk management approach
Sound management of information security and digital risk remains a top priority as the Group continues its digital transformation efforts. This focus is crucial in light of the evolving cyber threat landscape, which is further intensified by factors such as malicious threat actors using generative AI for deepfakes and phishing, as along with the increased risk of cyber-attacks associated with ongoing geopolitical conflicts.

Our information security and digital risk framework is supported by a robust set of policies, processes, and controls. It sets out a comprehensive approach to governing and managing associated risks. In addition, our enhancement programmes seek to continuously strengthen our overall technology and cyber resilience, enabling the Group to prepare for, respond to, and recover from any unforeseen IT disruption or cyber-attack. It encompasses regular assessments of key risk areas while considering various factors such as past incidents, regulatory requirements, and emerging threats. This risk-based approach enables the Group to better prioritise enhancements and risk mitigation efforts on key hotspots. Additionally, Senior Management and the Board are regularly updated of risk profiles, key trends, and any incident with significant impact across group-wide entities.

- **Key components of technology and cyber resilience**
  Preventive, detective and response capabilities
  A defence-in-depth approach is implemented featuring multi-layered controls and processes, along with regular reviews and testing of existing controls. New capabilities are added as needed to address evolving threats. Our 24/7 Cybersecurity Operations Centre and Technology Command Centre continuously monitor our networks and systems for potential cyber threats or disruptions to financial services. Enhancement programs are in place to strengthen our existing resiliency measures, ensuring robust technology and cyber risk management across the Group.

  Incident response and crisis management
  The scale and severity of events with potential cyber security threats are assessed, as they could impact the Group and lead to data loss or service disruptions. The Cyber Security Incident Response Team (CSIRT) is responsible for containing and eliminating these threats, as well as recovering from incidents to minimise the impact on essential financial services.

  Regular testing of IT disaster recovery (DR) plans is conducted to ensure their effectiveness in restoring critical system(s) promptly in the event of an incident. This testing also identifies opportunities for enhancements to further strengthen the existing DR plans. Additionally, regular cyber-related simulations (e.g., walkthrough of cyber incident and response) alongside crisis management exercises are performed to continuously assess the effectiveness of established processes and controls. These activities aim to enhance the preparedness of senior management in responding to potential cyber threat.

- **Other key aspects of information security and digital risk management**
  Information security capabilities
  Data loss prevention (DLP) controls are in place to minimise data loss events through web and email channels. Staff access to systems are granted on a need-to-know basis, and monitoring capabilities are implemented to detect potential abuse of authorised system accesses by staff.

  Awareness and vigilance uplift and testing programmes
  All employees are required to participate in mandatory cyber and information security awareness training, which is complemented by regular risk awareness broadcasts and social engineering testing programs. To enhance employees' knowledge, skills, and behaviours related to cyber security, the Group has implemented a Cyber Smart Programme that incorporates gamification and seminars.

  For selected employees, a Cyber Certification Pathway has been introduced to elevate their technical competencies in cyber security. Additionally, regular security advisories are provided to customers to increase their awareness and vigilance regarding information security practices, aimed at protecting their sensitive information.

  Cyber and network security insurance
  Relevant cyber and network security insurance are in place to cover damages that may result from specific cyber-attacks and technology disruption scenarios, including cyber extortion and business interruption losses caused by security breaches or system failures.

  Collaboration with regulators and industry partners
  To exchange cyber threat intelligence, active engagements are held with regulatory agencies in Singapore, Malaysia, Indonesia, Mainland China, and Hong Kong SAR, as well as the Financial Services Information Sharing and Analysis Centre. We also actively contribute to industry committees and working groups, including the ABS Standing Committee on Cyber Security, to share updates on information security and digital risk. The Group also participates in industry-level cyber exercises to enhance preparedness, improve incident response capabilities, and foster collaboration both within the Group and with regulators.