Risk Management

At OCBC, our approach to risk management underpins operational resilience, supports sustainable business growth, and promotes consistent long-term value creation for our customers, shareholders, employees, and communities.

Risk Landscape

Operating in an environment of geopolitical tensions, macroeconomic uncertainty and sector-specific headwinds, the Group maintained a proactive and vigilant risk management approach across the various risk types, in particular credit, operational resilience, third party arrangements, technology and cybersecurity domains. We conducted comprehensive stress testing to identify vulnerable customers, implemented targeted strategies for at-risk accounts, rebalanced our loan portfolio away from weak sectors, and intensified recovery efforts. Simultaneously, the Group leveraged on the Bank's operational and technology resilience frameworks to proactively manage and mitigate the impact of technology outages and third-party interruptions on our customers. Our multi-layered cybersecurity defences effectively safeguarded against evolving cyber threats. Collectively, these initiatives underscore the Group's commitment to long-term resilience and sustainable growth, closely aligning with the Bank's comprehensive management of principal risks such as credit, operational, information security and digital risk, as well as other interconnected risk areas.

Risk Management Approach

Risk ownership is a shared responsibility between the business units and risk functions as well as other support functions. The Group's leadership actively fosters a strong risk culture and sets a clear tone from the top, emphasising risk awareness, accountability, and ownership at every level. This commitment drives our comprehensive and disciplined risk management approach, which addresses all types of risks (financial and non-financial) and upholds the highest ethical standards. We identify risk sources and drivers, set risk appetites and tolerances aligned with business goals, and manage potential impacts under adverse circumstances. Risks are identified, measured and monitored using comprehensive metrics, on a standalone and aggregated basis, with a strong focus on early risk identification and mitigation, and pivoting our risk strategies in response to cyclical and structural changes.

Our risk frameworks define governance structures, roles and responsibilities, with well-documented policies and procedures for taking and managing risks. As risks are increasingly inter-connected, we adopt a holistic approach to risk assessment. Cross-functional teams identify and assess top and emerging risks using stress testing and scenario analysis to evaluate potential impacts of plausible risk factors on our earnings, capital, liquidity, customer segments and obligations. These insights shape our risk strategies and contingency plans.

We invest in our people and technology to ensure that the right skills, data, systems and infrastructure are in place to support effective risk management.

Principal Risk Types

Risks are categorised into five principal risk types, each managed with the appropriate expertise, resources, systems, policies and procedures. Our business, risk and functional support teams work together to actively identify, measure, approve, monitor, and report risks. Limits and triggers are set to ensure timely review and decision-making at appropriate authority levels. We also review our frameworks regularly to incorporate best practices and meet regulatory requirements in all countries where we operate.

Table 1: Principal Risk Types

Principal Risks	Definition
Credit Risk	The risk of financial loss due to a borrower/obligor 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 resulting from inadequate or failed internal processes, people, systems, or from external events. It covers a range of non-financial risks, including fraud, money laundering, terrorism financing and sanctions risk, third-party risk, physical security risk, conduct risk, business continuity risk, regulatory risk and legal risk.
Information Security and Digital Risk	The risk of data loss, financial loss, or disruption to financial services due to data leaks, cyberattacks or technology failures.

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

Risk Management

In addition to the five principal risk types, the Group considers environmental, social and governance (ESG) and climate risks, as well as responsible use of artificial intelligence (AI), given their increasing relevance and potential to influence the Group's risk profile across multiple risk dimensions.

Environmental, Social and Governance (ESG) and Climate Risks

Managing ESG and climate risks is vital to our operations, as they can impact other principal risk types such as 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. We have also taken steps to enhance our understanding of nature-related financial risks as we recognise the need to manage environmental risks holistically, and the increased saliency of nature degradation.

For more details on our initiatives, please refer to our Sustainability Report 2025 on Climate Action and Responsible Financing.

Responsible Use of Artificial Intelligence (AI)

The Group continues to explore and identify opportunities to embed AI across key use cases to deepen data insights and support decision making. These aim to improve productivity and operational efficiency, uplift customer experience, and enhance risk management processes.

As we expand AI adoption across the Group, we remain vigilant of the associated risks and committed to ethical and responsible AI deployment with close oversight. We recognise that threat actors are increasingly exploiting AI through deepfakes, sophisticated malware, and advanced phishing techniques, creating new avenues for fraud against the organisation and our customers.

To address these challenges, we maintain a robust governance framework supported by policies and guardrails to ensure proper oversight on ethical and responsible AI use. Strong controls are in place to identify, manage and mitigate potential harm from AI misuse. We also continue to collaborate with industry stakeholders to strengthen our frameworks, recognising the fast-evolving nature of AI and its regulatory landscape and the need for collective action. This disciplined approach reflects our commitment to continuously innovate with integrity – harnessing AI to deliver value, capture new opportunities, and uphold trust and accountability.

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. It 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 outlined on page 83.

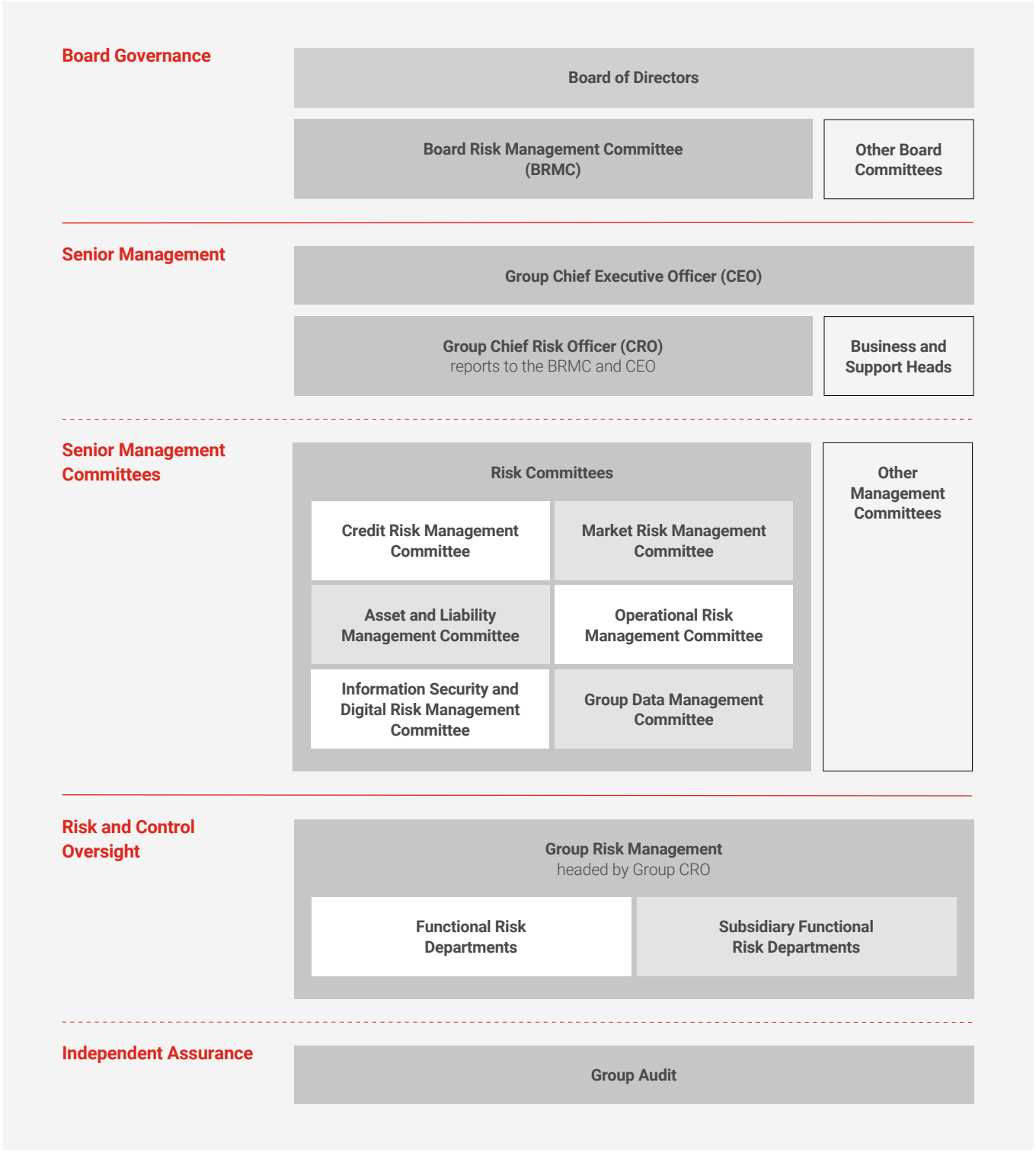
The Board Risk Management Committee (BRMC) oversees all risk management matters and ensures that our enterprise-wide risk management philosophy, principles and risk appetite align with the corporate strategy. The BRMC has oversight of credit, market, liquidity, information security and digital, operational, conduct, money laundering and terrorism financing, fraud, legal, regulatory, strategic, ESG and fiduciary risks, as well as any other risk category delegated by the Board or deemed necessary by the BRMC.

The BRMC provides quantitative and qualitative guidance to major business units and risk functions on risk-taking. Together with senior management, it regularly reviews risk drivers, profiles, frameworks and policies, and compliance matters. For more details, please refer to the Corporate Governance Chapter.

Senior management from risk-taking and risk control functions form dedicated functional risk committees to facilitate close risk oversight and governance. These committees are supported by the functional risk management units under the Group Risk Management Division (GRM).

GRM, led by the Group Chief Risk Officer (CRO), provides independent risk control and manages credit, market, liquidity, information security and digital, operational and ESG risks. The Group CRO is a member of the Group Management Executive Committee and functional risk committees. GRM delivers regular risk reports, monitors material risk drivers, identifies 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 to ensure the Group's long-term viability. The Board sets 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 consider the corporate strategy, the forward-looking operating environment and potential risks assessed against our risk appetite. We operationalise our risk appetite across the Group through our policies, processes, systems and limits to manage financial and non-financial risks. Together, these components form our Risk Appetite Framework, which articulates Group-level risk appetite 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 meet regularly to review macroeconomic and financial developments, discuss operating conditions and event risks, and potential 'dark clouds' that may significantly impact our earnings or solvency. These risks are measured via stress tests as well as sector/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.

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 adopts a proactive strategy to oversee credit risk across the Group's lending business, setting clear objectives and minimum standards. We apply a disciplined, balanced approach to manage credit risks and mitigate potential losses as we support sustainable, quality growth of our credit underwriting activities. The framework defines credit approval authorities, concentration limits, risk-rating methodologies, portfolio review parameters and guidelines for managing distressed exposures.

We manage risk through a combination of expert judgment and data-driven insights. Credit specialists apply their expertise to manage the risks of different portfolios and customer segments. All credit exposures require approval by credit approving officers, with approval authority levels delegated to officers based on their experience, seniority and track record. Specific policies and procedures that govern major customer segments are in Table 3.

Table 3: Credit Risk Management Approach for Major Customer Segments

Consumers and Small Businesses	• Evaluate credits using established program lending parameters, a structured risk-return framework and targeted customer selection criteria. • Employ advanced credit models for consistent credit decisioning, minimise deviations from credit criteria and escalate any exceptions for review to maintain robust risk controls. • Enhance portfolio oversight by leveraging advanced analytics, behavioural models, and regular stress testing to identify emerging risks and potential weak credits for timely intervention.
Corporate and Institutional Customers	• Conduct thorough individual credit assessments through independent evaluations by experienced credit risk managers, adhering to target market and risk acceptance criteria, and base decisions on detailed qualitative and quantitative analyses including a range of rating models. • Ensure joint credit approvals between business and credit risk units for objectivity, while conducting regular portfolio 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, adhering to 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 using stress tests to proactively identify potential issues early.

Counterparty Credit Risk Management

Counterparty credit risk arises from the potential default of a counterparty, borrower or obligor during our trading and/or banking activities including derivatives and debt securities. We measure counterparty credit exposure based on both current replacement cost and potential future exposures arising from market price fluctuations. This risk also includes 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.

Counterparty credit risk is managed across multiple dimensions at both individual and portfolio levels. The Bank uses a Potential Future Exposure (PFE) model to measure potential credit exposure arising from traded derivative products. The PFE model provides a quantitative estimate of potential future credit exposure movements driven by market rates, prices, and volatilities at certain confidence level over different time horizons based on transactions tenure. This forward-looking model, based on Monte-Carlo simulation and full revaluation, aligns with regulatory expectations, enhances risk transparency and optimises credit limit resource utilisations.

Risk Management

Credit Risk Mitigation

Credit risk is mitigated through various measures such as holding collateral, buying credit protection and setting netting arrangements to reduce credit risk exposures. These measures complement and do not replace our proper assessment of the obligor's ability to repay, which remains the primary source of repayment. Our credit policies define eligibility criteria for 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 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 used 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. Where possible, we clear Over-the-Counter (OTC) derivatives transactions through approved central clearing counterparties, replacing the counterparty's credit risk with that of a highly regulated and better credit rated central clearing counterparty.

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). These arrangements require 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.

Securitisation Exposures

We may arrange securitisation transactions for distribution and/or invest in such transactions arranged by the Bank or by third parties. In addition, we may act as a liquidity provider, credit facility provider, or swap counterparty. The risks relating to securitisation transactions adhere to our risk management policies and procedures. All investment decisions undergo an independent risk assessment and approval process, and approved investments are recorded in the banking book. We review credit limits regularly to ensure prudent risk management.

Securitisation exposures in both the banking and trading books are risk-weighted according to the approaches prescribed by MAS Notice 637. We continuously monitor the size and risk profile of these exposures and enhance our risk measurement processes as needed.

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, general corporates, corporate real estate (including income producing real estate) and other specialised lending portfolios such as project finance and object finance.	• 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 remaining specialised lending portfolio (i.e. 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.

Other Credit Risk Models

In addition to IRB models, we have been progressively developing and deploying other types of credit risk models such as Transaction-score models and Early Warning models for better risk management purpose, using alternate data and machine learning methods.

- **Portfolio Reporting**

This encompasses both internal and external reporting of portfolio risk information to the respective stakeholders. These reports offer valuable insights into the evolving trends of credit portfolio risk 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.

- **Portfolio Management**

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.

These portfolio insights are also applied to identify and quantify more vulnerable segments and take proactive, appropriate risk management actions, especially during periods of high uncertainties and volatility (e.g. slow economic growth, high inflation, elevated interest rates, and heightened trade and geopolitical tensions). The credit risk management actions include proactively identifying and 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

Credit policies and processes are established to identify vulnerable borrowers early. We proactively monitor credit portfolio quality and discuss emerging risks at dedicated risk forums, where we discuss, develop and review risk management action plans to address deteriorating trends.

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

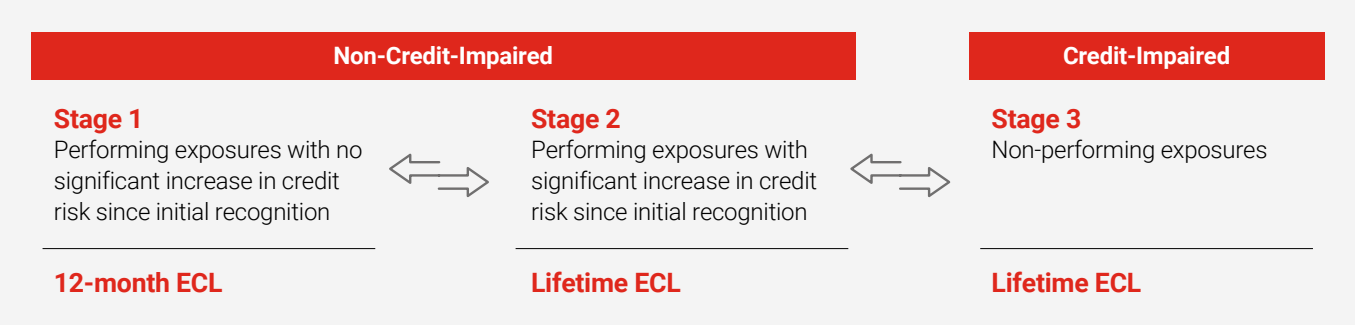
Dedicated remedial management units manage the restructuring, workout, and recovery of non-performing assets (NPAs) for wholesale portfolios. The aim is to rehabilitate NPAs where possible or maximise recoveries for NPAs under exit strategies. For retail portfolios, we apply risk-based and time-based collections strategies to maximise recoveries while minimising 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.

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

Table 5: Trading Portfolio VaR by Asset Class Risk

	2025				2024			
SGD Million	**End of the period**	**Average**	**Minimum**	**Maximum**	End of the period	Average	Minimum	Maximum
Interest Rate VaR	**5.2**	**8.7**	**1.3**	**18.6**	6.3	6.9	4.4	10.8
Foreign Exchange VaR	**3.3**	**2.5**	**0.9**	**10.4**	2.8	2.3	0.8	8.0
Equity VaR	**3.5**	**3.8**	**0.8**	**8.0**	3.6	2.5	0.8	4.3
Credit Spread VaR	**1.6**	**2.5**	**1.3**	**5.3**	2.0	2.8	1.7	4.6
Commodity VaR	**1.4**	**0.3**	**0.0**	**2.3**	0.0	0.4	0.0	1.7
Diversification Effect[1]	**(8.2)**	**(9.9)**	**NM[2]**	**NM[2]**	(9.5)	(8.6)	NM[2]	NM[2]
Aggregate VaR	**6.8**	**7.8**	**3.6**	**12.7**	5.2	6.3	4.1	10.6

[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.

Traded Market Risk

Traded market risk is the potential impact to the Bank's earnings or capital due to adverse movement in market rates and prices.

- **Measures**

  Value-at-risk (VaR) quantifies market risk exposures arising from our trading portfolio activities. VaR is measured and monitored by the different asset class risks, 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 2025 and 31 December 2024.

  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, Present Value of a One Basis Point Move in Credit Spreads (CS01) and other risk measures for specific exposure types.

- **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 can undertake authorised trading activities only for approved products. We monitor all trading risk positions 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 also manage market risk exposure holistically by using multiple market risk limits (VaR and market risk sensitivities), P&L Stop-Loss and other measures. We report exceptions, including temporary breaches, promptly to Senior Management, the relevant risk committee(s) and the Board.

  Model Validation

  Model validation is an integral part of our risk control process. Financial models are used to price financial instruments and calculate risk measures. 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 and hypothetical trading P&Ls daily to confirm that the model does not underestimate our market risk exposures. Our trading portfolios registered five back testing exceptions, mainly driven by heightened market volatility following a series of global trade tariffs imposed by the United States in April and May 2025. These exceptions remain within the threshold of the VaR model.

Designation of Trading Positions

We comply with the regulatory guidelines in designating trades as trading positions. The designation is primarily based on our intention for short-term resale, to realise gains from price movements, or to engage in price arbitrage. In certain cases, listed equities are designated to the banking book due to strategic objectives; such exceptions have been duly approved by the regulator. We maintain robust governance processes to monitor and report any transfers between trading and banking books. In addition, trading positions are subject to regular reviews to identify and address stale positions that exceed our internally prescribed holding periods.

- **Market Risk Weighted Assets**

  We adopt the Standardised Approach to compute market risk regulatory capital under MAS Notice 637 for trading book positions. Under MAS Notice 637, Internal Risk Transfer is established to facilitate transfer of interest rate hedging risk from the banking book to the trading book through a designated portfolio. This ensures that there are capital savings only when risk is transferred externally. With Internal Risk Transfer activities established, we consolidate interest rate risk hedging requirements and reduce counterparty exposure in the banking book through dedicated portfolios across various geographical locations.

  For Credit Valuation Adjustment, we apply the reduced version of the Basic Approach for Credit Valuation Adjustment (BA-CVA) which does not recognise hedges for computation of capital requirements.

Interest Rate Risk in the Banking Book (IRRBB)

Our Banking Book manages the cash flows originating from loans and deposits and maintains an inventory of bonds to meet our liquidity needs and regulatory compliance. With a broad range of products across different interest rate structures, curves and maturities, mismatches in asset and liability repricing profiles can occur. Changes in interest rates and yield curves may affect our capital and earnings.

The Group Asset and Liability Committee (ALCO) provides stewardship and regularly reviews our IRRBB profiles to ensure alignment with our business strategies and risk appetite, taking into account prevailing macroeconomic and market developments.

- **Measures**

  IRRBB is managed using both earnings- and capital-based measures.

  Net Interest Income (NII) sensitivity estimates the potential earnings impact under various interest rate scenarios, assuming our 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 interest rate shocks on our capital by discounting repricing cashflows, including commercial margins and spreads, using risk-free rates or appropriate proxies.

These measures take into account the impact of loan prepayment and fixed deposit early redemption, which are modelled referencing historical customer behaviour, product features and market indicators. For non-maturity deposits without explicit maturity or repricing dates, the repricing profile is determined by studying the elasticity of deposit rates against market interest rates and the volatility of deposit balances. These modelling assumptions are independently validated, reviewed and approved by Group ALCO and applied consistently for public disclosure and internal risk monitoring purposes.

- **Stress Testing and Scenario Analysis**

  We conduct regular stress tests across historical, hypothetical and regulatory interest rate shock scenarios as well as internal scenarios, to assess the potential impact of adverse interest rate movements on our financial position. These assessments serve as critical inputs for shaping interest rate risk profiles and management strategies.

- **Risk Monitoring, Reporting and Control**

  Interest rate risk positions and metrics are computed at least monthly and 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.

Structural Foreign Exchange (SFX) Risk

SFX exposures arise from non-Singapore Dollar investments in overseas branches, subsidiaries, other strategic investments and property assets. These exposures affect our Capital Adequacy Ratio (CAR), and total equity through the impact on Foreign Currency Translation Reserves. We monitor the SFX impact on our capital and CAR stability and conduct regular stress tests to ensure that potential losses under severe market stress scenarios remain within our risk tolerance.

Other Risks

We transfer most non-structural foreign exchange exposures in our banking book to our trading book for foreign exchange risk management. In addition, we are exposed to credit spread risk from holding High-Quality Liquid Assets (HQLA) in our banking book to meet the liquidity and regulatory requirements. While our HQLA holdings carry low default risk, their value can be sensitive to credit spread changes. We monitor this risk against approved CS01 limits on a daily basis and conduct historical and forward-looking stress tests. Another risk in our banking book is equity price risk arising from our equity investments in listed and unlisted companies.

These equity investments (excluding those held by GEH) form an insignificant portion of our overall securities portfolio.

Liquidity Risk Management

Liquidity risk is the risk of the Bank being unable to meet its financial obligations as they fall due without affecting daily operations and incurring unacceptable costs or losses.

Liquidity Risk Management Approach

The aim of liquidity risk management is to ensure that the Group can meet its financial obligations and support new business opportunities by effectively managing liquidity and funding risks within our risk appetite. This involves maintaining a diversified funding base and holding sufficient liquid assets to meet liquidity needs under both normal and stress circumstances, while balancing cost efficiency.

To achieve this, the Group has implemented a comprehensive liquidity risk management framework and policies that establish consistent guidelines and standards across jurisdictions. The Group ALCO oversees and regularly reviews our liquidity risk profiles to ensure they remain aligned with our business strategies and risk appetite.

- **Measures**
  Liquidity risk is assessed by projecting cash flow mismatches using both contractual and behavioural assumptions under normal conditions and stress scenarios. We monitor concentration level and regulatory liquidity ratios to evaluate funding diversification and resilience, with early warning indicators in place to detect potential liquidity risks stemming from market developments.

- **Stress Testing and Scenario Analysis**
  We conduct regular stress tests under a variety of adverse scenarios to assess the potential impact of idiosyncratic and market events on our liquidity risk profile. These outcomes inform funding strategies, liquidity policies and contingency funding plans to minimise the impact of any liquidity crunch.

- **Risk Monitoring, Reporting and Control**
  We continuously monitor liquidity risk positions against approved liquidity risk limits and triggers, aligned with our risk appetite and regulatory requirements. Rigorous review and oversight processes are in place to facilitate prompt escalation and remediation of any limit exceptions.

Operational Risk Management

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, systems, or from external events.

Operational Risk Management Approach

Our operational risk management framework defines how we manage and control operational risks arising from our business activities and operations. The framework is supported by various programmes that ensure preparedness and minimise the impact of adverse events 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, including operational risk events, key risk indicators, material issues and trends. The Board also receives an annual assurance report on the adequacy and effectiveness of our internal controls and risk management systems.

A key focus area is Operational Resilience which 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, including those provided by third parties. We proactively anticipate and prevent potential operational risk events through robust risk management practices.

Our Operational Resilience strategy builds on existing programmes such as business continuity management, crisis management, third-party risk management, technology risk management and cyber security. The robust risk management practices adopted by these programmes enable us to anticipate, prepare for, respond to, recover from, and learn from disruptive events.

- **Key Aspects of Operational Risk Management**
  Business Continuity Management
  Business Continuity Management ensures the Bank can maintain critical services during disruptions, minimising downtime and safeguarding customers and assets. The programme identifies Critical Business Services, sets Service Recovery Time Objectives, and maps supporting processes, systems, third-party service providers and other critical dependencies to develop detailed business continuity plans for various scenarios. Annual exercises are conducted to test and validate readiness and effectiveness of strategies. In addition, recovery and resolution plans are integrated to enable an orderly restoration of operations.

  Third-Party Risk Management
  Third-Party Risk Management addresses the risk of service disruption and other risks such as breaches of confidential information or non-compliance from the third parties. The Third-Party Risk Management programme includes a stringent onboarding process for third-party service providers, ongoing monitoring and periodic due diligence assessments. These measures help reduce the risk of service disruption, data breaches and non-compliance.

Incident Response and Crisis Management

Incident Response and Crisis Management involve a structured whole-of-bank approach for handling disruptive events such as public disorder, crime, terrorism, natural hazards, technology failures, cyberattacks and third-party outage. To ensure preparedness and effectiveness, procedures and protocols are established and regularly validated through crisis simulations, and industry-level exercises.

Physical Security Risk Management

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

Our physical security programme provides the foundation for a safe and secured environment for both customers and employees. In-house and external security experts conduct regular assessments, supported by continuous monitoring of emerging threats. Additionally, periodic physical security penetration exercises are conducted to maintain vigilance and preparedness of our security personnel.

New Product Review and Approval

The New Product Review and Approval prescribe a stringent review process for each new product or channel (including variations) to identify and mitigate 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

The Group has programmes in place to focus on appropriate incentive structures and regularly reviewed indicators related to employee's conduct. Surveillance programmes are in place to govern and drive risk management actions. The Board, through the Ethics and Conduct Committee, exercises active oversight on fair dealing, accountability and consequence management related matters.

Fraud Risk

The Group adopts a zero-tolerance stance against fraud, bribery and corruption. All instances of suspected fraud, bribery or corruption events are treated seriously and addressed 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.

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

Anti-Money Laundering (AML) / Countering the Financing of Terrorism (CFT)

The Group maintains a comprehensive AML/CFT control framework, anchored in sound governance, well-defined policies, and rigorous procedures, complemented by advanced risk detection tools. Robust risk surveillance capabilities, powered by AI and data analytics, enable agile monitoring and detection of suspicious networks, evolving financial crime trends and emerging 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 insurances comprising the Comprehensive Crime and Professional Indemnity, Directors and Officers Liability, Cyber and Network Security Liability are in place to cover key non-financial risks.

Information Security And Digital Risk Management

Information security and digital risk is a business risk comprising three risk domains - information, cyber and technology risks. Sound management of these risks is key to ensuring the confidentiality, integrity and availability of our information and critical systems. This approach minimises material impact on our customers and businesses from unforeseen events and align with regulatory expectations.

Information Security and Digital Risk Management Approach

Sound management of information security and digital risk remains a top priority as we continue to advance in our digital transformation journey. The cyber threat landscape is becoming increasingly sophisticated, with adversaries exploiting AI for deepfakes, malware-generation and phishing, alongside a growing number of targeted attacks on critical infrastructure and service providers in the region. These developments underscore the importance of maintaining strong cyber resilience to safeguard our stakeholders' interest.

Our information security and digital risk framework is supported by a comprehensive set of policies, processes, and controls that guide the governance and management of associated risks. We continue to invest in enhancement programmes to strengthen our technology and cyber resilience, including plans to engage a technology and cyber expert panel to advise senior management and the Board on a regular basis. We are highly focused on improving our capability to anticipate, respond to, and recover from unforeseen IT disruptions or cyberattacks with the objective of achieving operational resilience in serving our customers.

The programmes include regular assessments of key risk areas, referencing past incidents, regulatory developments, and emerging threats. Through this risk-based approach, we are able to prioritise mitigation efforts and focus enhancements effectively on areas of elevated risk exposures. Senior Management and the Board are regularly kept informed of risk profiles, key trends, and incidents across the Group. Additionally, the Board will be attesting to the MAS on a biennial basis regarding the adequacy of the Bank's internal controls and risk management practices to fulfil specific regulatory requirements.

- **Key Components of Technology and Cyber Resilience**

  Preventive, Detective and Response Capabilities

  A defence-in-depth approach is adopted, incorporating multi-layered controls and processes to safeguard our environment. These controls are subject to regular reviews and rigorous testing to ensure continued effectiveness, with new capabilities introduced as needed to address evolving threats. Our 24/7 Cybersecurity Operations Centre and Technology Command Centre provide continuous monitoring of networks and systems, enabling early detection of potential cyber threats or disruptions to financial services. Complementing these efforts, targeted enhancement programmes are in place to reinforce resilience and ensure robust technology and cyber risk management across the Group.

  Incident Response and Crisis Management

  A robust cyber security framework is established to proactively manage and respond to potential threats that could cause data loss or disrupt critical services. Our dedicated Cyber Security Incident Response Team plays a pivotal role in swiftly containing and eradicating threats, while ensuring timely recovery from incidents to minimise impact on essential financial services.

  To maintain operational resilience, we regularly conduct IT Disaster Recovery exercise to validate recovery capabilities and identify areas for improvement. Cyber-related simulations (e.g., tabletop and cyber range exercises) and crisis management exercises are also performed regularly to assess response effectiveness, uplift staff competency and enhance senior management readiness.

- **Other Key Aspects of Information Security & Digital Risk Management**

  Information Security Capabilities

  Data Loss Prevention controls are implemented to mitigate the risk of data leakage through channels such as web and email. Staff system access is governed by a strict need-to-know principle, ensuring that access rights are limited to what is necessary for their roles. In addition, monitoring mechanisms are in place to detect and flag any potential misuse of authorised access, reinforcing accountability and safeguarding sensitive information.

  Awareness and Vigilance Uplift and Testing Programmes

  To foster a strong culture of cyber awareness and vigilance, employees undergo mandatory cyber and information security training, supported by regular risk awareness broadcasts and social engineering testing programmes. Our Cyber Smart Programme further reinforces this by combining gamified learning experiences with expert-led seminars to deepen understanding and encourage secure behaviours. For selected relevant roles, we have introduced a structured Cyber Certification Pathway to build advanced technical competencies in cyber security. At the same time, we send customers periodic security advisories to keep them informed and vigilant in protecting their information.

  Cyber and Network Security Insurance

  Relevant cyber and network security insurance are in place to mitigate potential losses arising from specific cyberattacks and technology disruption scenarios, including cyber extortion and business interruption caused by security breaches or system failures.

  Collaboration with Regulators and Industry Partners

  The Group collaborates actively with regulatory authorities in Singapore, Malaysia, Indonesia, Mainland China, and Hong Kong SAR, as well as the Financial Services Information Sharing and Analysis Centre to facilitate timely exchange of cyber threat intelligence. We play a leading role in facilitating timely threat intelligence sharing and strengthening the financial industry's collective preparedness. The Group also participates in national-level cyber exercises to enhance technical readiness and foster deeper collaboration with regulatory bodies.