

# Governance, Risk Management and Compliance

Operating under constant economic, social, and environmental changes, the Bank believes that determination and commitment to transparent corporate governance, proactive risk management, and strict compliance with relevant laws, rules, and regulations are crucial components in building a strong organizational foundation and creating a competitive advantage for sustainable growth.

## Corporate Governance

Corporate governance is the foundation of organizational management that operates with ethics, integrity, and responsibility, leading to stakeholder trust and sustainable growth. The Board of Directors assigned the Nomination, Compensation, and Corporate Governance Committee with tasks to formulate the Bank's corporate governance policy and monitor compliance, as well as review and make appropriate changes to the policy in order to comply with regulatory requirements and global practices.

# 01

## Board of Directors



The Board of Directors is responsible for monitoring implementations and compliance with the specified policy to ensure that the Bank has an internal control mechanism that would effectively and continuously manage, assess and monitor the implementations. This system takes fair business practices, transparency, and responsibilities to stakeholders governed by the principles of corporate governance into account for long-term value creation to the Bank.



# 02

## Fostering Diversity



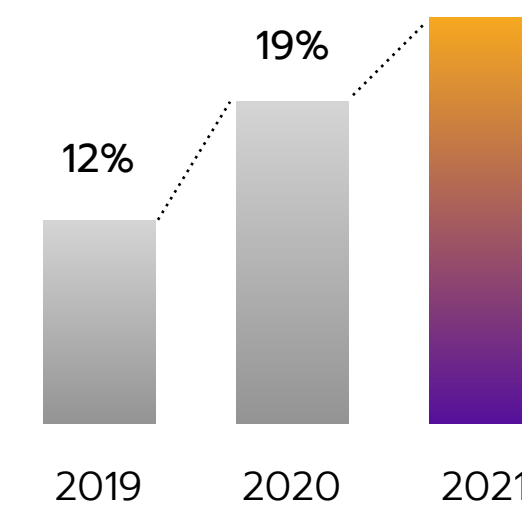
By recognizing inclusivity and diversity as key mechanisms in supporting business operation under the context of social change, the Bank places significance on nomination criteria and selection process of highly qualified directors that incorporate diversity factors, including, gender, race, nationality, age, educational background, professional experience, skills, knowledge, and other legal and societal aspects. This is to promote diversity of the Board of Directors that would bring a greater breadth of perspectives and opinions, benefitting all stakeholders and driving sustainable growth.

Accordingly, for director nomination and selection, the Bank screens qualified candidates based on nominations submitted by shareholders and directors and with consideration to the directors' pool. The board skill matrix is also applied to the assessment of the skills and expertise of directors to ensure the right fit for the Bank's strategy and business direction while taking into account diversity factors elaborated above.



# 24%

of SCB directors are female



# 03

## Encouraging Board Effectiveness



To ensure effective governance under the leadership of the Board of Directors, apart from establishing a robust structure of governance, carrying out the nomination and selection process, and allocating an appropriate compensation scheme for the directors, the Bank also encourages directors' responsibility by specifying Board meetings to be organized at least six times per year, and at least once in 3 months interval. Each director is required to attend at least 75% of the total number of meeting in a given year.

Moreover, Board and Committee's assessment is conducted annually and is divided into four parts, including 1) Board assessment, 2) Board committees assessment, 3) Individual director assessment, and 4) Board and chairman assessment. Self-evaluation and cross-evaluation are also conducted by the Bank on an annual basis, and by a third party once every three years or as deemed appropriate.

**Remark:** More information and performance on SCB corporate governance is reported in the 2021 One Report.



In 2021, 13 Board meetings were organized. The meeting attendance of the Board was 99%, The attendance of all 17 directors was above 75% of total meetings organized, which is in line with the Board charter.



All four parts of Board and Committee's 2021 assessment results were 'Excellent'.



## Risk Management

The Bank continues to develop a robust risk management process by specifying risk management as a fundamental component in every business process, coordinated at every level while promoting a bank-wide risk culture under effective risk governance and internal control systems.

# 01

## Risk Governance



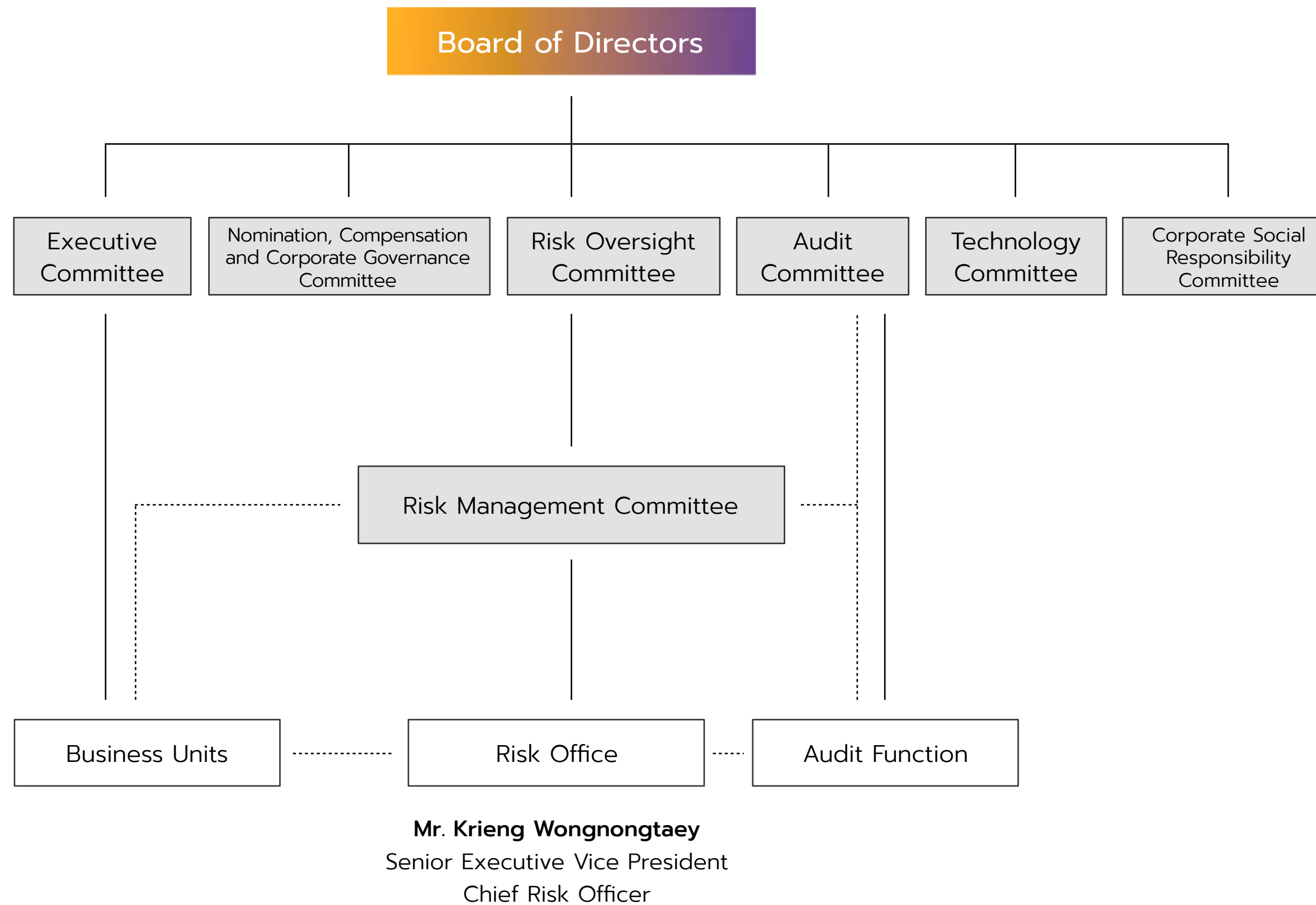
At SCB, risk management is specified and integrated into every business process with governance bodies overseeing the identified risks and coordinated on every level from the director, management, to operation level.

In addition, the Board of Directors is responsible for reviewing and approving the Bank's key risk management policies and appointing sub-committees to manage risks: Risk Oversight Committee formulating risk management strategies that are aligned with overall risk management framework, as well as screening, reviewing, monitoring compliance with overall and adequacy of policies and approaches in place. At the same time, every business unit is also accountable for identifying and controlling risks, assessing the adequacy of internal control mechanisms in order to collectively and effectively manage risks.

 **Director Level**

 **Management Level**

 **Execution Level**



Furthermore, the Bank places importance on continuously enhancing risk management knowledge and capabilities of the directors by producing monthly reports with key risks trends, risk events, and mitigation measures. Training by both internal and external experts are also provided periodically.

In 2021, directors participated in training on the topic relating to the Bank’s key risks such as Cyber Armor: Capital Market Board Awareness training on the topic of Capital Market Threat Landscape, Cybersecurity and Intelligence Threats Assessment, arranged by Thailand Securities and Exchange Commission Office, and Cyber Resilience Leadership: Herd Immunity, arranged by the Bank of Thailand in cooperation with Securities and Exchange Commission Office and Office of Insurance Commission.



# 02

## Emerging Risks



The Bank annually analyses emerging risks resulting from economic, social, and environmental changes which may affect business operations in the long-term. Appropriate measures are then put in place to effectively mitigate and manage the risks. In 2021, the Bank identified 4 following emerging risks:

- Risks from climate change and approaches to achieving Carbon Neutrality
- Cybersecurity risks from increasing reliance on digital technology and adoption of new business model and operation
- Epidemic and Dangerous Contagious Diseases
- Geopolitical Risk



## Risks from climate change and approaches to achieving Carbon Neutrality

### Importance

SCB has closely monitored the global coalition and the commitment of financial institutions worldwide to reach Carbon Neutrality 2050. In this regard, Thailand took an important milestone in 2021 when the government joined the 26<sup>th</sup> UN Climate Change Conference (COP26) and pledged to accomplish Carbon Neutrality by 2050 with provision of support on finance and technology as well as international cooperation. Since the new goal is 15 years earlier than Thailand’s initial Carbon Neutrality commitment by 2065, the Bank has then examined

potential transition risks which could emerge ahead of the plan, particularly regulatory changes and government policy to mitigate GHG emissions. Similarly, modern markets and technology will focus on high-capability and environmentally-friendly alternatives in transition to a low-carbon and green economy. Under such circumstances, certain projects not aligning or supporting a decarbonization target might face constraints as well as adverse impacts on asset values and operating costs due to regulatory changes, especially the fossil fuel industry and heavy GHG emitters.

Furthermore, the Bank consistently monitors physical risks from climate change which could have impacts on the economy –from the slowdown of economic activities to business interruption; property damages; and shortfalls and degradation of natural resources, farm crops, and commodities.

Aside from that, SCB also monitors the EU Carbon Border Adjustment Mechanism (CBAM) to help clients reshape their business plans and stay competitive in the global market.

**Impact to the Bank**

Given potential regulatory shifts towards GHG management, there might be long-term impacts on project finance of which business model or technology does not align with the Carbon Neutrality target.

Moreover, since project finance receives a longer repayment period than other loan products, there are higher risks of stranded assets that could significantly damage the Bank’s revenue and performance. Certain projects with high risks are heavy polluters such as coal mining and unconventional petroleum production.

SCB recognizes that the Carbon Neutrality ambition could deter competitiveness of companies that face constraints in adopting clean technology or reshaping business

models to accommodate the target both within firms and along the supply chain. Any regulatory changes or financial measures related to GHG reduction will likely affect the business performance and expansion strategy of SCB clients, thus causing ripple effects onto the Bank if we end up failing to present financial solutions as planned.

**Management Approach**

Considering the estimated impacts, SCB adopts the Equator Principles, which require every large-scale project finance—with high environmental impacts and annual GHG emissions of over 100,000 tons of carbon dioxide equivalent—to undergo and report climate risk assessment both in terms of transition and physical risks. By doing so, any

project finance developer will be made aware of potential environmental impacts and thus able to identify appropriate solutions and concrete management plans.

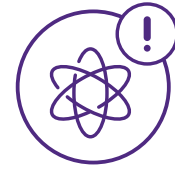
For general business, SCB has continued to offer loans to clean energy businesses and low-carbon infrastructure projects. As the world and Thailand took further steps on GHG mitigation to meet the Carbon Neutrality commitment, the Bank also started to develop wide-ranging financial solutions and loan products to assist our clients in their journey to a low-carbon transition. The Bank offers solutions in the form of loans and financial products such as derivatives—all subject to industrial standards ranging from the Green Bond Principles to the Sustainability-Linked Bond Principles.

Most recently, SCB became the first financial institution in Thailand to launch the ESG-Linked Interest Rate Swap in 2021.

Moreover, the Bank plans to review projects and companies in its portfolio exposed to high-risk industries in order to identify appropriate measures such as reducing the proportion of such industries, consulting with clients on GHG emission approach through low-carbon projects.

[For more details on SCB approaches to promote a transition low-carbon economy and climate-related risks management to achieve the Carbon Neutrality commitment, please visit “Sustainable Finance” on page 40-48 and “Climate Risk and Resilience” on page 84-85.](#)





## Cybersecurity risks from increasing reliance on digital technology and adoption of new business model and operation

### Importance

Today's business landscape has forced companies—including SCB—to heavily rely on technology as a key business driver. Cybersecurity risks thus become inevitable and even more evident in the wake of COVID-19 outbreaks, which prompted the Bank to shift from onsite to remote work. The Work from Anywhere arrangement could pose risks to the security system as it allows more convenient access to Bank's internal system and data.

Risk management and proactive measures to ensure cybersecurity thus play a pivotal role in strengthening cyber protection and preventing damages in case of unfavorable events such as infrastructure shutdown, service disruption, security breach, and personal data theft. In particular, the Bank has employed the Cybersecurity Mesh Architecture, which emphasizes building cybersecurity and expanding coverage beyond SCB premise to anywhere, that is, extending cybersecurity controls anywhere needed.

### Impact to the Bank

Increased reliance on digital technology as well as the adoption of advanced data management and storage system could imperil the SCB's position against cybersecurity risks. As the Bank strives to enhance digital platforms and data networks with partners, such unfavorable conditions would affect not only SCB but also our clients and business partners.

Cyber risks might result in financial damage, worsening reputation, and loss of trust from clients and

other stakeholders—including the regulators who could impose a penalty on the Bank.

For customers, cyberattacks could cause inconveniences due to system disruption, whereas data privacy abuse and misuse might result in financial damages.

Meanwhile, cyber risks would threaten business partners' confidence in the Bank's system security, internal management, and business operation, thus negatively affecting decision-making on current and future partnerships.

### Management Approach

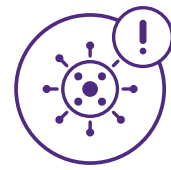
To level up the security of our operations and digital platform, SCB has increased the share of investment in infrastructure, tools, and cybersecurity technology based upon the 'Three-Line of Defense Framework.' The procedure is overseen by the IT and cybersecurity governance structure –comprising the Technology Committee and operating officers. In addition,, SCB has an internal Cyber Intelligence Unit to examine and monitor cyber threats—from type to feature, trend, and case study—to develop and maintain modern and efficient response procedures. The Cyber Intelligence

Unit works closely with the Security Operations Center who is tasked with responsibility for scrutinizing access to SCB network and IT system as well as preparing to counter cyberattacks in a timely manner.

As the Bank becomes more exposed to cyber risks due to the Work from Anywhere arrangement, SCB adopts the 'Cyber Security Mesh Architecture' to create a collaborative ecosystem of security tools. The model ensures end-to-end security points to both onsite and remote work; the tasks are connected and monitored through a centralized aggregation point.

In addition, all business partners and suppliers are required to undertake a cybersecurity risk assessment before commencing work with SCB, in order to determine their readiness and necessary risk management approaches. By doing so, the Bank can ensure that every access and transfer of data proceeds in compliance with prudent standards and management approaches while recognizing and managing cybersecurity risks.

[For more details on SCB cybersecurity risk management, please visit "Cybersecurity" on page 128-129.](#)



## Epidemic and Dangerous Contagious Diseases

### Importance

In today’s era where the world—people, technology, news, and data—intertwines through a seamless connection, novel disease outbreaks have inevitable impacts on economic, social, and political stability. Throughout the past two years, the COVID-19 pandemic has led to wide-ranging effects such as:

- The global economy entering a recession
- Exacerbating social inequality in terms of income distribution, access to healthcare, and adaptability
- Rising unemployment and uncertainties
- Financial fragility of small entrepreneurs and swelling household debt
- New threats such as fraud, cybersecurity, and data privacy

Furthermore, the pandemic has brought about the New Normal where all stakeholders—from personal to organizational, societal, and national levels—must seek approaches and collaborative efforts to embrace the new global paradigm.

### Impact to the Bank

As one of the epidemic and contagious diseases, the COVID-19 pandemic has affected the Bank’s operation in various aspects such as:

**Business Operation:** The Bank might fail to meet a target performance if the economy falls into a recession. Meanwhile, virus control measures have prompted the Bank to reshape our business strategy. Furthermore, our current business model may unlikely

to fulfill customer demand or expectation in the New Normal era where coronavirus outbreaks forever change consumer behavior and way of life. Therefore, SCB must develop a new business game plan to pursue sustainable growth ahead.

**Customer Service:** The COVID-19 pandemic has also accelerated digital transformation, as evident in a rapid increase in the number of consumers adopting online financial transactions during the outbreaks. In response, the Bank must continue to enhance service capacity to facilitate a seamless transaction while ensuring data security and privacy to deliver a distinct customer experience with the highest satisfaction.

**Credit Quality:** Loans—the largest contribution in SCB assets—are facing higher risks of debt service default as corporate clients in some industries and regions are confronted with income and profit shortfalls, whereas some have been operating at a deficit. Also, there could be more potential debt defaults among retail borrowers as the unemployment crisis continues.

**Employee Care:** SCB has introduced the Work from Anywhere arrangement to increase workforce flexibility during the pandemic. Therefore, the Bank needs to enhance IT system capacity to ensure that SCB employees at head offices and branch networks can still work efficiently while maintaining access to skill development and learning courses.

**Management Approach**

As the post COVID-19 pandemic remains highly uncertain, it is of paramount importance for the Bank to formulate policy responses against arising challenges and uncover innovation to uplift business resilience in the New Normal era after the outbreaks subside. To do so, the Bank has in place key risk management policies which consist of the followings:

**Business Operation:** SCB actively prepares and rehearses Business Continuity Plan to ensure readiness and service continuity in case of emergency and, at the same time, reshapes our business model and strategy in efforts to stay buoyant in the new business paradigm. In

2021, the Bank announced the establishment of SCB<sup>x</sup>, which reflects our aspiration to march beyond traditional banking services and ride on financial strength to fully transform into FinTech business and platform of the future. [For more details on the establishment of SCB<sup>x</sup>, please visit "Special Report" on page 16-19\).](#)

**Customer Service:** SCB Digital Bank (DBank) was established as an internal unit that focuses on digital business growth and strategy to strengthen access and meaningful relationship with our customers. DBank leverages AI technology and expansive database to present tailor-made financial solutions that cater to each client's demand and condition. The Bank also strives to

protect customer data privacy at the highest standards, thus adopting the Cybersecurity Mesh Architecture –which aims to build and extend cybersecurity controls anywhere needed and beyond the Bank's premises. [For more details on SCB cybersecurity risk management, please visit "Cybersecurity" on page 128-129.](#)

**Credit Quality:** SCB places emphasis on assessing impacts upon credit portfolios in a timely manner. The Bank must be able to identify affected debtors from each situation that might deteriorate overall credit quality and find approaches to control, monitor, and report risks to executives. In addition, SCB maintains sufficient monetary reserves in case of

urgency and regularly conduct scenario analysis to ensure that current assessment models are practical to any circumstance.

**Employee Care:** SCB prioritizes taking care of employees and ensuring safety in all aspects. Our employee cares to include enforcing the Work from Anywhere policy as a permanent arrangement; providing essential work devices and tools; uplifting cybersecurity measures to global standards; providing alternative vaccines to employees at all levels; organizing activities to uplift physical and mental health; and offering financial assistance to employees affected by the COVID-19 outbreaks.





## Geopolitical Risk

### Importance

Geopolitical risk is a risk arising from tension between nations due to political situations, conflicts, scramble for natural resources, terrorism, threat from weapon of mass destruction, which could be escalated to regional and global levels. Geopolitical risk can transmit to economic sectors via investors' confidence and sentiment, and economic activity. In a time of geopolitical stress, the tension affects overall confidence and results in investment volatility, slowdown or stagnant economic activity, or acceleration toward economic recession.

### Impact to the Bank

The Bank is aware of geopolitical risk and potential impact associated with credit risk. As Thailand heavily relies on import of raw material and intermediate goods and export products to foreign countries, and with a significant number of customers in the Bank's portfolio operate in import/export sector, manufacturing, transportation, and supply chain. Political tension in one country or between nations could negatively impact cash flow and performance deterioration of businesses, and their ability to meet financial obligations while demands for

financial products for import/export business decline. If the situation becomes more severe or prolonged, it could accelerate the economic crisis and unemployment. These affect creditworthiness of business and retail customers of the Bank.

### Management Approach

Recognizant of potential impacts resulting in geopolitical risk, the Bank establishes effective and proactive risk management process to ensure that the risk is appropriately assessed and monitored by embedding geopolitical risks in the credit decision process and credit review

to ensure that the credit decision is forward-looking. In addition, the Bank controls country risk by setting limits on lending, investment, and contingent liabilities for each country. SCB's Country Risk Management Policy requires both direct and indirect country-specific exposure to be included when calculating the country-risk limits. When situation arises or becomes intensified, the Bank promptly assesses the impact on the portfolio and conduct stress test to ensure that the Bank has sufficient provision and capital to mitigate potential losses



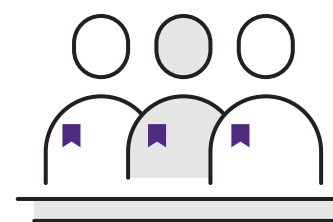
# 03

## Cultivating Risk Culture



The Bank adopted “Hong Kong Monetary Authority Bank Culture Reform” framework to guide its risk culture implementation from Governance, Incentive System, and Proactive Reporting Measures to drive shared risk and management responsibility throughout the organization.

### Governance



Risk Oversight Committee is responsible for providing consultation to the Board of Directors on cultivating a risk awareness culture throughout the organization and corporate culture compliance.

### Incentive System



The Bank identified risk management as part of the Balanced Scorecard, aligning with executives’ and employees’ performance appraisals in each business unit. The Bank also organized risk-related engagement activities such as Best Operational Risk Champion Award, Best BCP Coordinator Award, and Risk Culture Award.

### Proactive Reporting Measures



Risk reporting channels through Risk Governance Compliance (GRC) system and [whistleblower@scb.co.th](mailto:whistleblower@scb.co.th). The reported risks are then collected, analyzed, and reported to relevant committees.

By understanding that risk management is a duty of every employee, the Bank continues to build employees' engagement on the matter on the basis of knowledge, comprehension, and collective responsibilities through organizational management approach and activities that seek to foster and embed risk culture into everyday operations.

**Core Value**



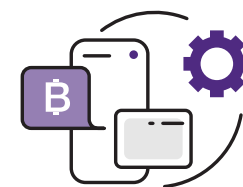
Specifying risk culture as one of the four SCB's core values, in which People Office continues to communicate and promote its behavioral compliance since onboarding, as well as integrating the value as part of a annual performance appraisals of senior executive. This is because SCB believes that leaders are key drivers to foster the desired culture through displayed behavior, role model and leading to bank-wide practice.

**Three Lines of Defenses**



Encouraging the adoption of "Three Lines of Defense" among the First Line (Business and support units), the Second Line (Risk Management and Compliance), and the Third Line (Internal Audit), while identifying risk assessment, mitigation measures, and monitoring.

**Product Development**



New Product Development Regulation requires product and/or process owners to holistically assess risks that may occur, and to seek approval per the specified risk level before developing or making any amendments, while ensuring to identify relevant risk control measures.

**Training**



Making 7 Operational Risks a mandatory training course, requiring every employee to participate and complete the course.

**Communication**



Apart from communication on policy and practice, directors and executives continuously communicate the importance of risk management and case studies of failure to comply with the Bank's rules and regulations, policies, and code of conduct to employees.











## Compliance with Laws, Rules, and Regulations

SCB is committed to communicating and building compliance with policies and procedures as well as with relevant rules and regulations by regularly reviewing, analyzing, and monitoring changes in the operating business context and relevant laws. This leads to continuous internal review, revision, and improvement of the Bank’s rules and regulations to ensure that business operations are aligned with relevant rules and regulations as well as global practices, contributing to solid and sustainable business conduct.

The Bank specifies 8 areas with significance to the Bank’s operation as mandatory courses.

### 8 Mandatory Courses, promoting a foundation of prudent and responsible business conduct

Course	Percentage of employees completing the course
 Personal Data Protection Act	97%
 Cyber Security Awareness	97%
 Anti-money Laundering and Counter Terrorist Financing	82%
 SCB Financial Group Code of Conduct	92%
 Operational Risk Management and Data Protection Handling	89%
 SCB Safety First	88%
 Anti-corruption and Bribery	87%
 Market Conduct	97%

# 01

## Committed to Ethical Business Conduct



The Bank is committed to operating its business with integrity and responsibility for all stakeholder groups by requiring directors, executives, and employees at all levels to strictly comply with the [SCB Financial Group Code of Conduct](#). The Audit Committee, which is made up entirely of independent directors, is responsible for overseeing compliance with the Bank’s principles of governance and ethics, code of conduct, regulations, and procedures, as well as regularly reviewing the Code of Conduct.

The Bank encourages our suppliers to adhere to the [SCB Supplier Code of Conduct](#), by requiring every supplier to sign an acknowledgment form before starting their work with the Bank. The content of the SCB Supplier Code of Conduct includes business ethics, respect for labor rights and human rights, occupational health and safety, environmental practice guidelines, and compliance with laws and regulations.

### Whistleblowing

Under the Whistleblower Guideline, the Bank provides channels to report information or tips about non-compliance with rules, regulations, and the Bank’s code of conduct, such as corruption and bribery cases. A fact-finding committee is responsible for promptly investigating any reported incidents or cases. Findings of any disciplinary decisions and subsequent actions are then reported to the Disciplinary Committee, which will then be presented to President, and Management Committee on a quarterly basis.

In 2021, there were a total of 48 reported incidents, 24 concerned non-compliance with procedures or obligations, 10 concerned discrimination and harassment, 5 concerned inappropriate behavior at workplace, 5 concerned dishonest conduct, 2 concerned mistakes in assigned tasks, and 2 related to a fraudulent act. Out of all the cases, 42 were investigated and addressed while the 6 remaining cases are still being deliberated. Additionally, the Bank has implemented appropriate disciplinary actions for affirmed cases, including written warnings, salary reductions, and employment termination. 1 case was given written warning in 2021 after being found guilty of the misconduct. The Bank encourages employees at all levels to report incidents or cases that may affect the Bank through the channels that have been set up, which will then trigger the investigation and review process.

### Whistleblowing Channels

- [whistleblower@scb.co.th](mailto:whistleblower@scb.co.th)
- Governance Risk Compliance (GRC) system on the intranet
- Mail to P.O. Box 117, Chatuchak Post Office
- Telephone: 0-2544-2000



# 02

## Anti-corruption and Bribery



The Bank pledges to shun and prevent any form of corruption and bribery by requiring every employee to learn and comply with the Bank’s [Anti-corruption and Bribery policy and practice](#), which is explicitly stated in SCB’s Financial Group Code of Conduct. The Bank is a declared member of Collective Action Coalition Against Corruption (CAC) since 2010 and become a certified member since 2017 to date.

At the same time, the Bank continues to enforce a No Gift Policy to demonstrate the Bank’s commitment to transparent business conduct, adhering to the code of conduct, and in compliance with the Anti-corruption and Bribery Policy.

Nevertheless, for political contributions in monetary or other forms, the Bank requires appropriate disclosure as well as approval from the Board of Directors or the Executive Committee. Violation and/ or failure to adhere to the policy will result in disciplinary action which, after an investigation according to the Bank’s disciplinary procedures, may involve written warning, termination of employment, or civil and criminal lawsuits.

In 2021, there were no corruption and bribery allegations or complaints against the Bank from the Bank of Thailand, the Anti-money Laundering Office, the Office of the National Anti-corruption Commission, and the Securities and Exchange Commission. The Bank also did not provide any support to political activities, political parties, politicians, election candidates, or people with direct or indirect political influence.





# 03

## Anti-Money Laundering and Prevention



The Bank specifies policy and procedures relating to anti-money laundering and counter-terrorism and the proliferation of weapons of mass destruction financing which is applied to employees at all levels while continuing to develop and improve internal systems and processes to keep up with the new operating context in a digital era and ensure compliance with relevant rules and regulations, global practices, and the Bank’s Code of Conduct. This is to protect the Bank from being victimized by criminals or terrorists through money-laundering or financing terrorism and the proliferation of weapons of mass destruction.

The Bank complies with laws and regulations on keeping customer’s documents and information relating to AML/CFT by restoring and destroying the documents after 10 years.

### Training

Apart from mandatory training on Anti-money Laundering and Counter-Terrorism and the Proliferation of Weapons of Mass Destruction Financing (AML/CTF), designed with online assessment that employee needs to complete annually, the Bank also organized training sessions conducted by internal legal and compliance managers and external experts in 2021.





### AML/ CTF mandatory training for all employees

Online mandatory training which employees at all levels must complete and review on an annual basis. The contents are designed by the Thai Baking Academy (TBAC) with case studies and self-assessment

**86% of employees completing the course**



### Training and refresher sessions by internal legal or compliance manager

Knowledge sharing sessions and training on AML/ CFT/ WMD to SCB and subsidiaries' employees, including overseas branch staff. The training cover different subjects, such as AML/ CFT business and banking leadership preparation for employees in financial sectors.

**5 sessions organized**  
**200 employees attended the sessions**



### Communication

Communication on new AML/CFT/WMD rules and regulations, and inform relevant business units and subsidiary companies of the name list per the UN Sanction Thailand List, as well as individuals identified with high money-laundering risks.



### AML/ CTF mandatory training for relevant personnel

Intensive six-hour online training, covering knowledge, relevant rules, and regulations of the Anti-money Laundering Office. Relevant personnel must complete the course before beginning the work.

**85% of employees completing the course**



### Training by external expert

In 2021, SCB participated in AML/ CFT trainings on topics such as

- Seminar on AML risk assessment organized by Anti-money Laundering Office, and Multi-disciplinary Program with relevant agencies to enforce compliance with AML Act.
- Compliance Officer for commercial banks delivered by Faculty of Law, Chulalongkorn University in collaboration with the Bank of Thailand and Thai Bankers Association

# 04

## Respecting Human Rights



Recognizing human value and dignity, SCB strives to respect and promote basic human rights as specified in the SCB Financial Group Code of Conduct, and to strictly comply with global practices by respecting and promoting the human rights of all stakeholders, including customers, employees, the community, and suppliers. The Bank's [Human Rights Policy](#) has adopted the UN Guiding Principles on Business and Human Rights (UNGPR) to guide organizational management and practices.

On a three-year basis, in 2020 SCB undergoes human rights due diligence assessment to identify, prevent, and mitigate human rights impacts as a result of its activities throughout the value chain. The results are summarized as follows:

### 3 Steps of Human Rights Risks and Impact Assessment

#### Scoping

Reviewing the identified risks within the geography of operation and peer benchmarking to determine industry risks, including reports from global civil society organizations and NGOs

#### Identification

Building engagement with internal stakeholders to collaboratively identify risks associated with the Bank's operations

#### Prioritization

Determining the level of severity and likelihood by using a matrix

### Human rights issues associated with the Bank's operations and throughout the value chain

#### AS A SERVICE PROVIDER



#### CUSTOMER PRACTICES

1. Data privacy
2. Mis-selling
3. Product discrimination
4. Product development

#### AS A LENDER



#### INVESTMENT AND BUSINESS PRACTICES

1. Labor rights
2. Land rights
3. Community rights

#### AS AN EMPLOYER



#### EMPLOYMENT PRACTICES

1. Workplace discrimination
2. Working conditions
3. Freedom of association, assembly, and collective bargaining

#### AS A BUYER



#### SUPPLY CHAIN MANAGEMENT

1. Labor rights
2. Community rights
3. Security personnel practices

### 3 Salient issues



#### Data privacy and protection



#### Mis-selling



#### Community rights in lending projects/ investee companies

### Mitigation action and measures for salient issues

Please see more details in the Data Privacy Protection chapter on page 126-127

Please see more details in the Market Conduct chapter on page 130

Please see more details in the Sustainable Finance chapter on page 40-42

For a complete report on the SCB Human Rights Risks Assessment, please [click here](#)

# 05

## Protecting Personal Data



The Bank upholds human rights and understands that privacy is one of fundamental human rights that need to be respected and such is one of the key operational risk issues of the Bank. Personal data management framework, identifying personal data protection as one of operational risks with group-wide risk management approach was then developed; governed by specified governance, policies, processes, and procedures systematically enforced in order to build and maintain trust from customers and stakeholders.

### Governance of Data Privacy Protection

The Bank specified governance structure that promotes collaboration from the Board of Directors, senior executives, to employee at operation level. Under this structure, the Board of Directors is responsible for reviewing and approving policies as well as monitoring compliance with the laws and regulations relating to personal data protection. Here, Risk Oversight Committee and Technology Committee are also tasked

with role and responsibility in screening and reviewing data and personal privacy framework to ensure its efficiency and applicability. Other steering committees, consisting of senior executives, promote best practices, study progress and encourage implementations in alignment with the Personal Data Protection Act, B.E. 2562 (2019).

### From Policy to Practice

SCB publishes [Privacy Notice](#) to inform customers and the general public while strictly enforcing Data Privacy and Protection Policy as well as information technology security policies throughout the organization. SCB employees and outsourced parties are required to fully comply with relevant policies and procedures, including protection, collection and management of customer, employee, and other data owner's information as specified by law. Appropriate measures for using, sending, or transferring personal data are put in place to prevent violation and abuse of personal information.

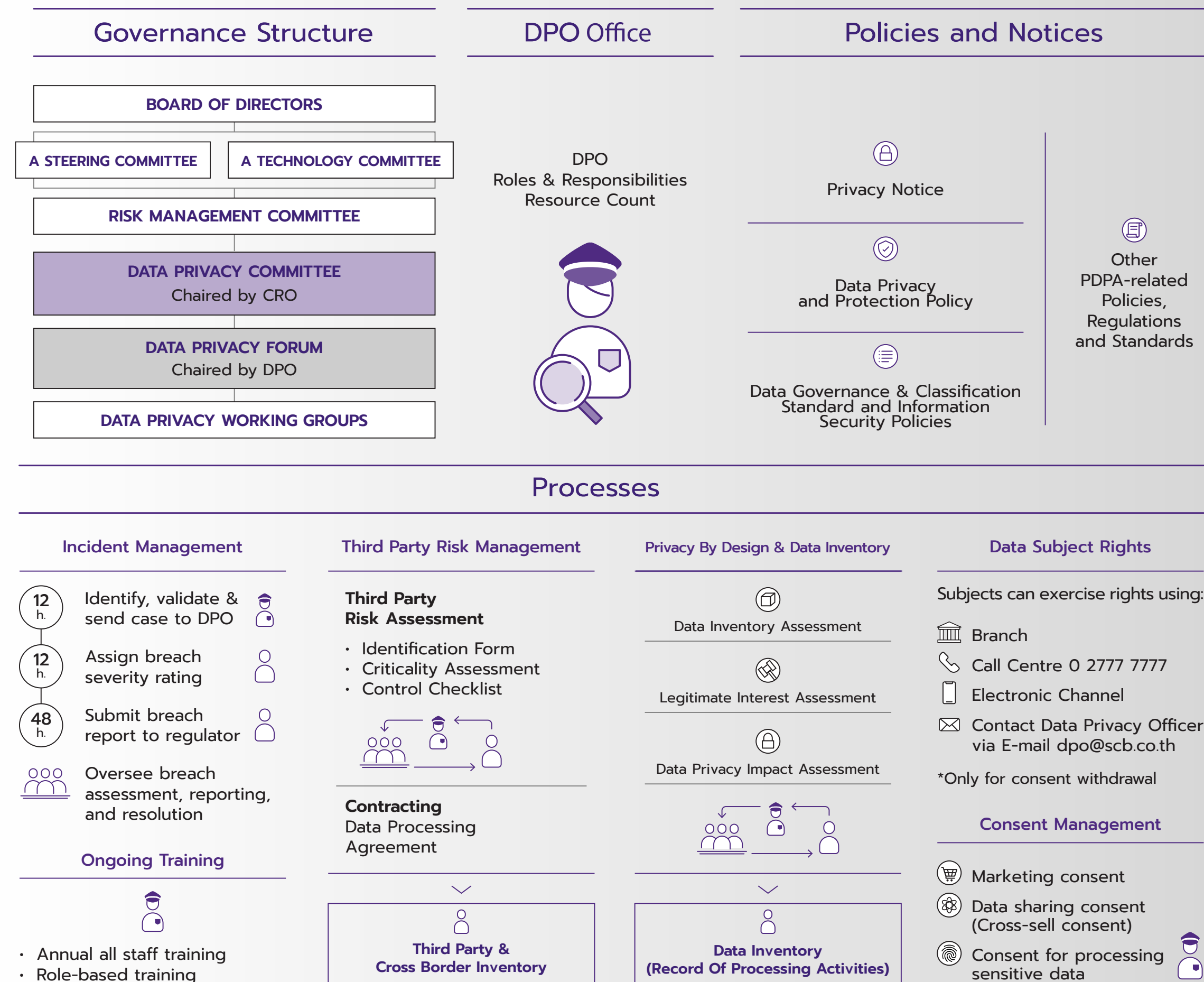
### Data Privacy Protection and Management

The Bank has specified privacy incident management procedures as a guideline for employees to effectively and appropriately handle and respond to a case of privacy breach. In addition, the Bank places importance on building awareness among employees through regular training, communication, and activities. Penalties, such as written warning, pay deduction, and employment termination, are enforced if employees are found guilty of personal data's violation or any mishandling that causes subsequent impacts. In 2021, the Bank received a total of 2 complaints regarding personal data violations, 1 of which is from the Bank's reporting channel, and 1 is from regulatory entity. In which the Bank has investigated and addressed the claims according to the Bank's procedures and practices. In addition, no personal data breach, theft, or loss was reported.



### Audit and Policy Compliance

Furthermore, in 2021, the Bank performed an internal audit on Data Privacy by internal audit team, in addition to commissioning an independent external audit company from 2019-2020 to assess its management and operation's alignments and compliance with the Personal Data Protection Act 2562 (2019). It was found that the Bank's practices and processes comply with the Act.



Bank-wide collaboration to ensure a desired state of privacy and to gain customers' trust. Governance, policies and processes in place to systematically operationalise data privacy measures.

**Remark:**

- The Bank enforces privacy notice, seeking cross-selling consents for marketing of product or services of SCB and its financial group companies, business partners which is aligned with PDPA, the Bank of Thailand's requirements while seeking consents relating to personal data/credit information per National Credit Bureau's requirement.



# 06

## Strengthening Cybersecurity and System Stability



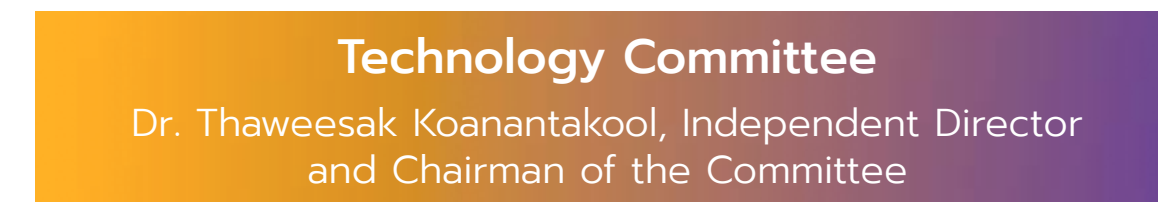
The Bank seeks to holistically uplift cybersecurity in terms of management, technology, and people while regularly testing its capabilities and the systems' readiness in effectively handling cyber threats or incidents. This is to ensure that the Bank can continuously operate business with robust information security system, network, and infrastructure which are of utmost security and stability to global standards, with sufficient resilience to effectively detect and respond to cyber threats.

### IT and Cybersecurity Governance

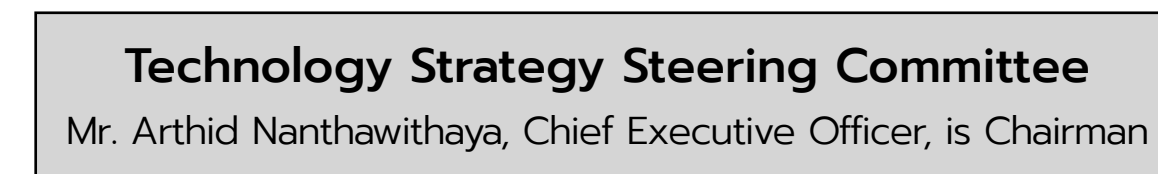
SCB governance structure on information technology and cybersecurity is classified into three levels, starting at director level, who appoints Technology Committee with roles and responsibilities in formulating long-term strategy, as well as integrating quality of service provision and technology risks management into the overall framework. At management and execution level, collaborative efforts are made to drive performance responding to policy and strategy specified by the Technology Committee.



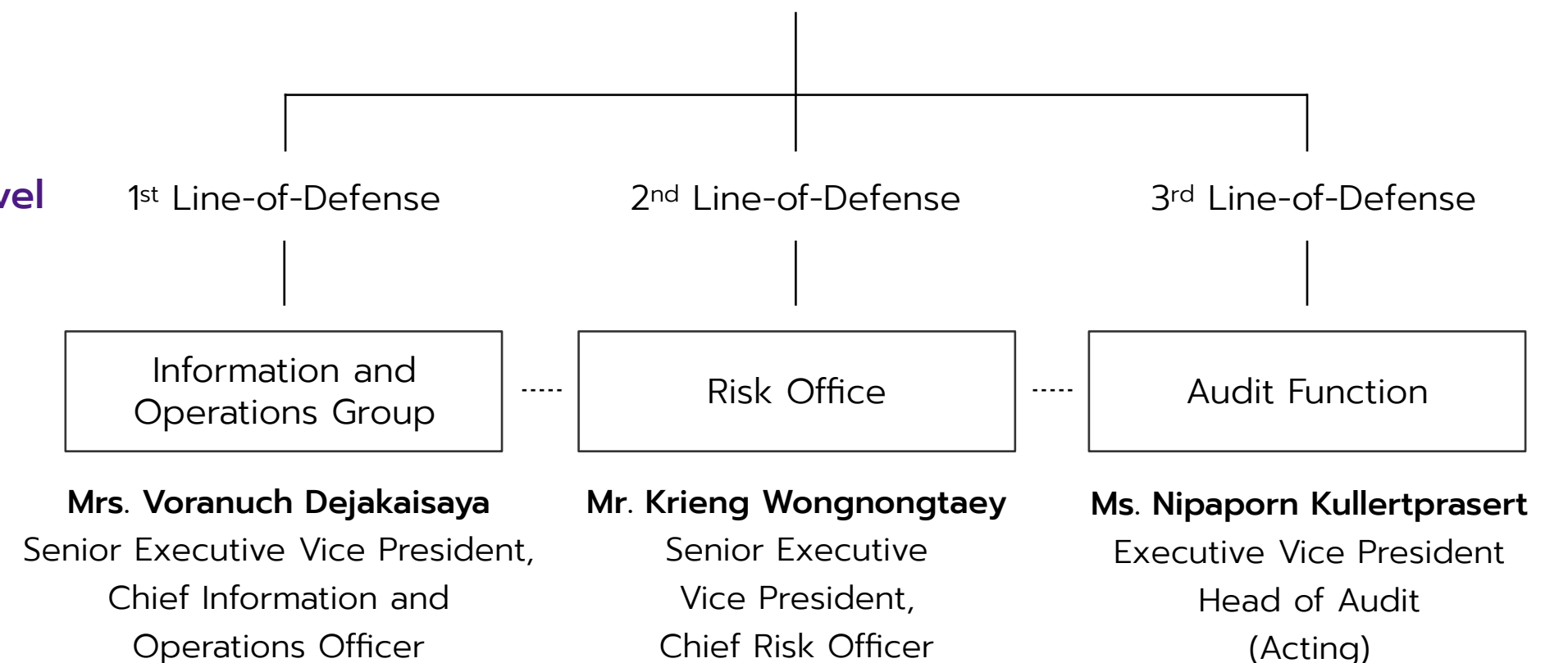
#### Director Level



#### Management Level



#### Execution Level



**Bank-wide Awareness**

SCB communicates IT and cyber security policies and standards to all levels of employees. Such information is readily available and accessible through the Intranet. In addition, along with year-round active awareness activities, mandatory training on cybersecurity are enforced and took many forms such as through gamification platforms and infographics. Moreover, for IT personnel, Technology Academy is established and responsible for building IT employee's capacity and awareness on IT-related risks in today's business context, while serving as a continuously learning/sharing community for IT personnel

In case of suspicious events relating to IT and cybersecurity, employees can report events or concerns through the actively-monitored channel, including e-mail to IT helpdesk, supervisor, or IT security department.

**Global Standards of Cyber Risk Management**

Having a robust, reliable, and resilient information technology system, network, and infrastructure are important for maintaining customer trust and ensuring business continuity. Accordingly, the Bank strictly enforces the Business Continuity Management (BCM) and Crisis Management Policy, as well as other relevant policies, including Cyber Security Incident Response Plan.

Moreover, the Bank also tests and rehearses readiness of such policies and plans in order to uplift capabilities and preparedness of relevant personnel. The tests cover technology and process response to various forms of cyberthreats including:

- Phishing stimulations - 2 types
- Red-Team Exercise and Cyberthreat Actor – 2 types
- Table-Top exercises with business units responsible for Cybersecurity Incident Response Plan – 1 time
- Surprise stimulation system recovery test – 1 time

Throughout 2021, the Bank performed at least 6 cyber-readiness tests with risk management functions. The results were then analyzed and reported to relevant committee for continuous improvement.

In addition, the Bank has been ISO/IEC 27001: 2013 for Information Security Management System: ISMS certified since 2005.

# 07

## Fair Consumer Practice



Fair treatment and access to financial services is a basic consumer right, the Bank is therefore committed to the Market Conduct principles while continuously developing and improving operations under the Zero Tolerance policy, or not deliberating any non-compliance in any form or case.

### Treatment of Vulnerable Customer

The Bank conducts business with the goal of providing every group of customers inclusive access to financial products and services, particularly for vulnerable customers who may require special care and assistance. At SCB, customers with the following characteristics are classified as vulnerable: those aged 60 years and older, those with limited financial knowledge or no investment experience, and those having communication, decision-making, or physical limitations. The Bank has an established procedure for treating vulnerable customers to ensure that these customers make fully informed

decisions when buying products and services. Here, the Bank requires a family member to be present during a sales presentation and sign as a witness. For customers with health issues that pose a limitation on communication and decision-making, two witnesses, one an SCB employee and the other a family member or physician, must be present at a sales presentation. Managers or supervisors must confirm understandings with customers and require written acknowledgment to ensure that customers receive accurate information and understand product or service before purchasing or agreeing to terms.