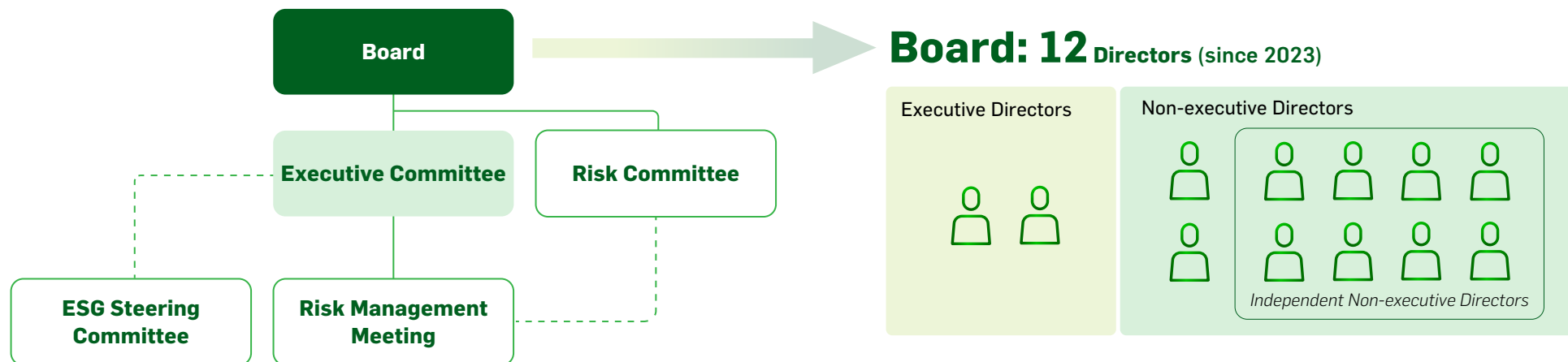


## ■ Being Proactive to Manage Risk

We have managed risks with the following management structure:



### Risk Management Framework

Managing risk is a core part of our day-to-day activities. We aim to protect our operations against compliance risks, and have a strong, transparent form of corporate governance. Our risk governance forums hold regular meetings to ensure our governance and control framework is properly discharged, managed, sustained and communicated. Besides, Our Chief Risk Officer represents the risk team on the ESG Steering Committee and leads the incorporation of climate risk into our risk management. Please refer to our [Annual Report 2022](#) to learn more about our bank-wide approach to risk.

### Three Lines of Defence model

We adopt the three lines of defence model to define the roles and responsibilities within the Bank. The activity-based framework delineates the accountabilities and responsibilities for risk management and the control environment within each line of defence. The model applies to all individuals and all risk types, including both financial risks (e.g., reputational risk, market risk) and non-financial risks (e.g., resilience risk), and supports the delivery of conduct outcomes.

**Clear segregation** between risk ownership (the first line of defence), risk oversight and stewardship (the second line of defence), and independent assurance (the third line of defence) is essential to help support effective identification, assessment, management and reporting of risks. Our activities, rather than our job titles, determine where we lie in the three lines of defence model.

**Global functions** may have responsibilities across both the first and second lines of defence, and therefore these responsibilities must be segregated across all teams. At an appropriate level of seniority (normally Executive Committee Member level or their direct reports), a single individual may have responsibilities across the first and second lines of defence. However, any such dual accountability cannot create unmanageable conflicts for the responsible person, particularly if they have regulatory accountability.

**Risk appetite** is defined as the level and types of risks that we are willing to take in order to achieve our strategic objectives. It is articulated through the risk appetite statement ('RAS'), which consists of qualitative statements and quantitative metrics covering financial and non-financial risks with the defined risk appetite and tolerance thresholds. Our RAS is approved by the Board and is subject to biannual review and regular monitoring.

## ■ Being Proactive to Manage Risk

**Risk reporting** enables the senior management and stakeholders to make informed decisions, by providing insightful analyses created from accurate and timely data, together with the perspectives of subject matter experts from across the three lines of defence. This risk reporting helps senior management to understand what the top risks are, and if they are managed within our risk appetite. It also provides visibility of the common themes and systemic issues across the organisation, which enables us to manage the risks more proactively and effectively.

**Internal audit** is the third line of defence, it provides independent and objective assurance as to whether the design and operational effectiveness of the Bank's framework of risk management, control and governance processes, as designed and represented by management, is adequate.

### Managing different types of risk

#### ESG risk management

In accordance with the HKEX's ESG Reporting Guide, the Board determines and evaluates the ESG-related risks that we face. The Bank recognises that effective management of ESG-related risks could help us shape a sustainable future and create long-term value for our stakeholders. Throughout the year, effective risk management and internal controls were put in place and reviews of these systems were conducted and confirmed by the management. The management also presented its confirmation of the effectiveness and adequacy of the Bank's disclosure framework, including its risk management and internal control systems relating to ESG to the Board for its confirmation.

#### Three Lines of Defence model

##### 3rd

Line of Defence

**Independent assurance**

##### 2nd

Line of Defence

**Risk oversight and stewardship**

##### 1st

Line of Defence

**Risk ownership**

During 2022, the Bank continued to formulate its ESG strategies, raised the level of staff awareness of the importance of and issues relating to ESG. It also continued to assist customers in transition to a low carbon economy, and strengthened its ESG disclosure to align with the latest regulatory requirements.

The Board has overall responsibility for the ESG matters identified by EXCO, based on the recommendations of the ESG Steering Committee, and for the integration of such matters into the Bank's strategies. ESG updates are provided to the Board at least twice a year, and the relevant key performance indicators are measured, monitored and reported to EXCO on

a quarterly basis. Meanwhile, ESG performance of the Bank and the relevant key performance indicators are measured, monitored and reported on a regular basis.

For HSVM, investee companies with low ESG scores are reviewed in the entity's ESG investment review meetings. Negative and exclusionary screenings are generally applied to all actively-managed portfolios under HSVM.

## ■ Being Proactive to Manage Risk ■ ■ ■ ■ ■

### Compliance

Our credibility relies on our operational integrity and the transparency of the information we provide to our stakeholders. Upholding strong corporate governance, adherence to the highest ethical standards and effective risk management are essential to being an accountable, transparent and well-managed company. Compliance issues are discussed and reviewed by the Board and management committees. As the body responsible for promoting our long-term sustainability and success, the Board provides forward-thinking leadership within a framework of prudent and effective controls. We are committed to maintaining quality, professionalism and integrity throughout our business operations. Internal controls, risk management, compliance, and legal and regulatory requirements are considered at our Board meetings.

In 2022, all Directors and staff undertook various training on values and conduct. This covered, among other topics, sustainability, risk management, cybersecurity, and anti-bribery and corruption. From time to time, further training is provided to our Directors and senior leaders. We require all our staff members to comply with the relevant codes of conduct. For details, please refer to the ["Staff code of conduct and staff awareness"](#) section.

NEDs attended NED Summits in March and September 2022. Topics of the Summits covered, among others, climate and energy security, net zero and sustainability policies. Directors also received a training on climate risk management in November 2022.

If the local corporate governance requirements are of a lower standard than our own, our higher standards of corporate governance practices shall apply (where they do not conflict with the law).

We perform horizon scanning for regulatory developments issued by the Hong Kong financial regulators, including the HKMA, SFC, IA, MPFA and other authorities supported by the Compliance Team. These include laws and regulations, circulars, codes, guidelines, consultations and consultation conclusions.

Regular reports on financial crime and regulatory compliance risk management are submitted to senior management governance committees.

The Audit Committee reviews our financial reporting, the nature and scope of audit reviews, the effectiveness of the systems of internal control and compliance relating to financial reporting, and the operation and effectiveness of whistleblowing policies and procedures.

Results of audit work together with an assessment of the overall risk management and control framework are reported to the Audit Committee and the Risk Committee as appropriate. The Internal Audit function reviews management action plans in relation to audit findings and verifies adequacy and effectiveness of the remediated controls before formally closing the issue.

No instance of non-compliance with laws and regulations that resulted in significant fines or non-monetary sanctions was recorded in 2022.

### Financial crime

We have a fundamental responsibility to help protect the integrity of the financial system on which millions of people depend. We are committed to only doing business with customers who meet our strict standards. We have ended relationships with customers where we felt that the financial crime risks were too great to manage effectively, and we continue to invest in the related expertise, partnership and systems.

As threats to the global financial system grow, we will continue to adapt our approach to aim to stay one step ahead. Over the coming years, we aim to make a step change in our effectiveness in fighting financial crime through intelligence-led financial crime risk management.

We have built a dedicated team of financial crime specialists and aim to equip our employees to speak up when something does not look right. Our dedicated Risk and Compliance function, led by experienced senior personnel, brings together all areas of financial crime risk management within the Bank.

We work in close partnership with law enforcement agencies to protect our customers. We are upgrading our systems to enable us to spot and analyse suspicious activities more effectively.

We are strengthening our defences against fraud. The global fraud landscape is characterised by increasingly sophisticated attacks targeting online banking and other digital services. Under our multi-year fraud transformation programme, we are investing in training our employees, as well as enhancing our technology-based defences.

## ■ Being Proactive to Manage Risk

We constantly strive to improve the ways that we detect and prevent financial crime and explore technologies that will help us build on our existing capabilities. Fighting financial crime is a key area that can benefit from innovation; therefore, we are working with, and investing in, a number of fintech firms that can help us achieve this.

We partner with local police to proactively tackle financial crime. Designated police hotlines are available for our staff to report instances of suspected fraud and forgery, in order to protect our customers from suffering financial loss. Designated emails are provided for the police, for the purpose of sharing the latest fraud intelligence with selected branches.

We uphold the standards that help ensure the Bank consistently operates ethically, honestly and with accountability. In 2022, our staff in Hong Kong received over 84,249 hours of learning on the topics of bribery and corruption, money laundering and sanctions, conduct, values and regulations.

We aim to ensure that our all staff are well-informed and vigilant regarding the detection and prevention of illicit and illegal activities, such as bribery and corruption, money laundering, sanctions and insider trading. All our employees are required to complete a learning programme on these subjects.

For frontline staff, we provide learning programmes on banking regulations, codes of practice and data privacy. Staff who work in high-risk roles receive additional, specialised learning regarding the detection and deterrence of financial crime.

Financial crime risk-related issues and progress are updated regularly and on a thematic basis to the relevant senior management governance committees, including the Executive Committee, Risk Management Meeting and Risk Committee.

In 2022, no judgements were entered against the Bank for failure to fight financial crime.

### Finance and tax risks

We principally operate and pay taxes in Hong Kong, where the statutory profits tax rate is 16.5%. Our average Effective Tax Rate ('ETR') is 13.1% which is lower than the statutory profits tax rate. We manage tax risk based on a formal management framework. We have adopted initiatives that increase transparency, such as the US Foreign Account Tax Compliance Act and the Organisation for Economic Co-operation and Development's ('OECD') Common Reporting Standard.

**84,249 hours**  
of learning on the topics of bribery and corruption, money laundering and sanctions, conduct, values and regulations received by our staff

We do not use tax avoidance structures or strategies, such as artificially diverting profits to low tax jurisdictions. We principally operate and pay taxes in Hong Kong, but we are committed to complying with the spirit and the letter of the tax law in all territories and countries in which we operate and to maintaining an open and transparent relationship with the tax authorities. Relevant financial information is disclosed in our [Annual Report 2022](#). We follow the tax policies and principles of HSBC.

Factors	Detail description	Effects on the ETR
Non-taxable income and non-deductible expenses	Mainly income from tax-exempt debt instruments (e.g. government bonds)	-3.4%
Others	Mainly tax deduction on Additional Tier 1 capital instruments	-0.3%
Share of losses / (profits) of associates	Exclusion of the tax effect of Hang Seng's share of net losses / (profits) from its associates	-0.03%*
Different tax rates in other countries / areas	Differential in the statutory tax rates between higher tax jurisdictions where Hang Seng also operates and Hong Kong (e.g. mainland China where the statutory tax rate equals to 25%)	+0.3%

\* The effect is immaterial

## ■ Being Proactive to Manage Risk

### Anti-bribery and corruption

We began a three-year programme in 2017 to advance the Bank's anti-bribery and corruption risk management capabilities. We have strengthened our controls and processes, and improved our global register for Associated Persons. The programme focused on enhancing our global gifts and entertainments register, which provides a consistent way to record, notify, approve and monitor gifts and entertainment. Dedicated personnel oversee anti-bribery and corruption compliance.

In the past five years, we made no contributions in any form to lobbyists, trade unions, or political organisations and campaigns.

We are committed to maintaining high ethical standards. Our policies on anti-money laundering, sanctions, and anti-bribery and corruption are aimed at ensuring that the risks identified by the Bank are appropriately mitigated.

For our policies on money laundering, bribery, corruption and sanctions, please refer to: <https://www.hsbc.com/who-we-are/esg-and-responsible-business/fighting-financial-crime/financial-crime-risk-policies>

Suppliers are required to agree to comply with the Ethical and Environmental Code of Conduct ('ECOC') for Suppliers of Goods and Services when they are invited for request for proposals or tendering, and when signing an agreement. This reminds suppliers the importance of our commitment to anti-bribery and anti-corruption. More than 300 suppliers signed the ECOC in 2022.

In 2022, there was no confirmed incident when contracts with business partners were terminated or not renewed due to violations related to corruption.



### Competition

Our Legal function is tasked with providing policies, guidance and training modules to help our businesses and functions understand and conduct their activities in compliance with the spirit and letter of Hong Kong's Competition Ordinance. This complements our ongoing training, through which our staff learn about the essential elements of competition law and how they apply to our business operations.

In 2022, no judgements were entered against Hang Seng for breaching the Competition Ordinance.

# Mandatory

for all our staff in Hong Kong, including contractors, to attend anti-corruption training

# 12 hours

anti-corruption training delivered to Directors in 2022



# 100%

of Directors received anti-corruption training in 2022

## ■ Being Proactive to Manage Risk

### Data privacy

The Bank continues to strengthen our data privacy policy, educates staffs on how to report security incidents and provides training on compliance in Hong Kong. Our cybersecurity experts investigate breaches and, if necessary, escalate matters to the major incident group. Specific processes for the handling and protection of our customer data are set out in an internal procedure manual. Our clear desk policy reduces the opportunities for unauthorised data access.

Data privacy is overseen by individual businesses and functions as first-line risk owners, while the Chief Data Officer is the first-line control owner. The Operational and Resilience Risk under Risk Department and Data Protection Officer provide second-line oversight. Officers at the functional and business units promote data protection and disseminate information on our guidelines and developments. (See Customer Privacy in [Our Customers](#))

Data Privacy Principles are set out to help manage data privacy risk.

**Four mandatory controls have been implemented since 2021, in order for us to practically manage the risks:**



#### Records of Processing

To understand identifiable data processed by the Bank, record the details of how the Bank processes such identifiable data, and keep evidence of the process, in order to make sure the Bank can demonstrate that it complies with data privacy Laws.



#### Internal and External Data Transfers

To make sure that any transfers of identifiable data are approved and compliant with the data privacy laws and the Bank's policies with respect to data privacy. This includes both internal transfers (transfers between HSBC entities in any jurisdiction) and external transfers.



#### Privacy Impact Assessments

To make sure that there is timely identification of data privacy risks arising from a new form of use, or a change in the processing, of the identifiable data, and to make sure that the risks identified are properly managed before the new form of use, or change in the processing of the identifiable data are enacted.



#### Data Disclosures

To make sure that external disclosures of identifiable data are processed in a timely, consistent, compliant and accurate manner, and in compliance with data privacy law. These disclosures are usually made in response to external requests.

Source	Customer privacy upheld* complaints
Outside parties	28
At the Bank	2
Regulatory bodies	0
<b>Total</b>	<b>30</b>

Type	Customer privacy upheld* complaints identified
Identified leaks	28
Thefts	0
Losses of customer data	2
Others	0
<b>Total</b>	<b>30</b>

\* Upheld means the cases are considered legitimate after an internal investigation.

## ■ Being Proactive to Manage Risk ■ ■ ■ ■ ■

### Cybersecurity

The cyber threat landscape continues to evolve at a fast pace, while controls designed to effectively mitigate cybersecurity risk will become outdated over time. Our stakeholders expect us to take the necessary steps in order to protect the markets, their data and business interests to the best standards. Over the years, we have invested in attaining the good practice standards for cybersecurity and we are committed to maintaining this position in the future.

**Ongoing review** on the cyber risk appetite and the ongoing effectiveness of our controls in mitigating these risks is needed, in order to maintain good practice standards under the dynamic environment with threats. While in most cases it is extremely difficult to reduce the potential impact of a cyberattack, it is possible, through an investment in ongoing controls, to reduce the overall likelihood of a cyber-risk being realised. A continued re-evaluation of the effectiveness and an investment in the maintenance and enhancement of the controls, can enable the Bank to keep the residual risk at an acceptable level.

**Ongoing investment** in our defence against ever more sophisticated cyberattacks are made. We have enhanced our event detection, incident responses, secure development, vulnerability remediation and protection against malware, application layer attacks and data leakages. We have also strengthened our third-party management by including cybersecurity due diligence, through which stricter governance and enforced third-party security testing prior to the approval of a contract.

**All the IT infrastructure** in our operations has adopted the industry-standard National Institute of Standards and Technology framework. Banks are high-profile targets for criminals seeking financial gain, personal information and disruption, which may potentially lead to financial loss, reputational damage and customers loss. Protecting our customers and the Bank from such threats is a key component in our strategy to become a connected business.

**Risk governance forums** such as the Board-delegated Risk Committee and Risk Management Meeting are regular meetings to ensure our governance and control framework is properly discharged, managed, sustained and communicated. To protect our operations against compliance risks, we have strong and transparent corporate governance measures in place.

**Regularly reporting** on our strategic programme and key indicators are conducted to support the Board and senior management's oversight of cybersecurity. Our cybersecurity strategy is reviewed and the business risk profiles, mitigation awareness, internal and external cybersecurity incidents, as well as the regulatory requirements are discussed.

**Cybersecurity drills** are also conducted with Board and senior management, to rehearse the types of decisions that may need to be taken and to reconfirm the individual roles and responsibilities during a major cyber incident. Periodical cyberattack drills are conducted to enhance the level of understanding in terms of the roles, protocols, internal communication paths and escalation procedures across the

business in the event of a cyberattack. Phishing tests are also conducted on a regular basis to raise the level of security awareness across the organisation.

**24/7 hotline** is available for our staff to report cybersecurity incident immediately at its occurrence. These incidents are handled by our cybersecurity analyst and Security Operations Centre, then they are reported to our management personnel to seek direction on the remediation. Cybersecurity incident response procedures have also been established and tested regularly.

**Cybersecurity training** with automated cybersecurity assessment tools are offered to all users, such as, executives and their assistants, IT end users, software developers, third-party service providers, etc. We adopt vulnerabilities across the network, operating systems, application layers and in-house custom software are managed through a centralised platform and are remedied according to the priority.

Throughout 2022, cybersecurity awareness and training regarding data security has been delivered to all staff including the security community on a regular or as-needed basis. It covered topics such as data security, email security and phishing, access control, incident reporting and escalation, secure use of communication devices and social media, information classification and labelling, etc.

## ■ Being Proactive to Manage Risk

Training or communication regarding cybersecurity offered in 2022 included:

- ▶ Mandatory e-learning for all staff
- ▶ Briefings to the Board and Executive Committee members
- ▶ Role-specific training for staff who play an integral part in the businesses and functions and have the responsibility to effectively manage their information security risks
- ▶ Training for executive assistants and IT staff
- ▶ Awareness sharing for all staff and their family members
- ▶ Seminars hosted by senior leaders which also featured expert speakers

**>99%** 

Employees who completed the mandatory cybersecurity training on time.

**>90%** 

IT developers who hold at least one of our internal secure developer certifications.

### Staff code of conduct and staff awareness

The Bank's staff code of conduct ('the Code') sets out the rules, regulations and standards of behaviour that all employees and contractors are expected to adhere to.

The staff code of conduct is available on our employee self-service portal in English and Chinese. All employees, including new joiners and contractors, are required to read the Code and complete an online curriculum for the Code to ensure their understanding on the rules and regulations set out in the Code.

We provide learning programmes on different behaviour standards outlined in the Code. Employees are required to complete the learning programme based on their roles.

In 2022, there was no identified material cases of non-adherence to our staff code of conduct involving regulatory compliance. Apart from reporting to relevant regulator(s) where appropriate, the Bank has been proactive in undertaking consequence management, depending on the severity level of the cases.

### Equal opportunities, non-discrimination and human rights

We are committed to promoting an inclusive culture. Our people managers are expected to create and foster a strong speak-up culture in their teams, where our staff can be confident that their views matter, that their workplace is free from bias, discrimination and harassment, and that their careers will advance based on merit. We uphold diversity and inclusion when hiring staff. Our recruitment process is merit-based and free from bias and discrimination.

To nurture an inclusive and speak-up culture, all our staff undertake mandatory training on our values and conduct. Workshops by legal professionals are arranged for the employees to be equipped with the knowledge and skills to handle discrimination, harassment and bullying. In particular, to support people managers in handling staff matters. Diversity learning is also embedded in the induction programme for new joiners.

The impact is demonstrated by a favourable inclusion index at 75% in our 2022 employee survey. 82% of our staff indicated that they believe that the Bank is committed to addressing bullying and harassment at work.



## ■ Being Proactive to Manage Risk

We believe that a diverse and inclusive workforce is critical to running a sustainable and successful business. Our approach aims to harness the benefits of diverse teams to drive greater innovation, enhance collaboration and improve workforce agility.

Our culture values, respects and supports individuals, where their richness of ideas, backgrounds, styles and perspectives are actively sought out with informed empathy to create business value.



Disciplinary action was taken against 1.3% of our employees due to poor conduct, for example, demonstrating poor sales conduct when conducted sales activities, use of inappropriate language. Three employees were dismissed for dishonesty behaviours.

The Bank's staff code of conduct also outlines our expectations on human rights matters. It is reviewed on an annual basis and when required to reflect the latest regulatory requirements and the Bank's internal policies. Any changes to the Code are submitted to EXCO for review and approval.

2% of the staff have reported they are with disability from 2022 Snapshot survey.

### Conflicts of interest

Stringent internal structures ensure that duties are appropriately segregated. For example, our investment frontline business and investment operations are managed by different departments to avoid conflicts of interest. Staff responsible for sensitive or high-risk areas are required to adhere to specific rules and to undergo training on how to avoid conflicts of interest.

### Whistleblowing

We are committed to providing our employees a safe and secure workplace. We value diversity and aims to create a workplace where individuals from varied backgrounds come together to deliver in a high-performance organisation, with equal opportunity for all.

Individual differences, be it interpersonal or more complex and related to organisational policy / decision(s), can arise in the workplace. Although most are resolved through engagement between employees and their managers in an informal setting, a formal grievance mechanism may be necessary to resolve more complex grievances.

We make every effort to ensure that our employees can raise concerns confidentially and without fear of repercussion. Retaliation against whistleblowers is not tolerated. We adhere to HSBC's whistleblowing policy and utilise a secure and confidential platform via which staff can raise concerns when the normal channels for escalation are unavailable or inappropriate. We also provide a number of speak-up channels, including reporting to managers, as well as escalation to HR, the Financial Crime Unusual Activity Report platform and our internal whistleblowing portal, etc.

Our internal whistleblowing portal is designed as a process to promote consistency in our controls, investigations, reporting, oversight and governance of all whistleblowing activities. With our internal whistleblowing portal, which is accessible through 24/7 hotlines and an online portal in multiple languages managed by independent third party, our employees can raise concerns confidentially, while employees may choose to make an anonymous report if they are not comfortable with disclosing their identities. All cases reported are treated confidentially as far as possible. All whistleblowing cases are investigated by the subject matter experts, in accordance with HSBC's policies and standards.

## ■ Being Proactive to Manage Risk

A well-established employee grievance procedure is in place. We make our best endeavours to ensure that investigations are carried out objectively in light of the information provided and that necessary resulting actions are taken. In 2022, 15 grievance cases were reported to HR through HR online portal.

At times, individuals may not feel comfortable speaking up through the usual channels. HSBC Confidential is our global whistleblowing channel, which is open to all our colleagues to raise concerns about wrongdoings and unethical behaviour. The Bank's policy is that staff members and others should be able to raise any matters of concern confidentially and anonymously. Therefore, appropriate steps should be taken to maintain that confidentiality.

Whistleblowing channels are stated in the section of HSBC's Supplier Management Conduct Principles and also at the whistleblowing policy. Suppliers can express their concerns via this email [hsbc.vendor.concerns@hsbc.com].

In 2022, there are 50 new whistleblowing cases received. By the end of the year, 42 cases were closed, including 31 cases raised during the same year.

### Business continuity planning

Business continuity and incident management policies are formulated with reference to HSBC's guidelines and the Bank's own circumstances. Our business continuity planning policy, pandemic guidelines and the major incident management plan are reviewed and updated on regular basis or upon lessons learnt from the actual incidents to provide clear guidance to the businesses and functions to plan on how to manage the contingency risk. The Bank's business resilience steering group ('BRSG') consists of senior management representatives and is chaired by the Chief Operating Officer to provide guidance and to ensure the effectiveness of our operational resilience capabilities. In discharging these responsibilities, Hang Seng senior management committee members will evaluate, approve, action or escalate resilience issues on resilience policy, capability and risks. The BRSG Pre-Group is formed to support the Hang Seng HK BRSG. The membership and responsibilities of the BRSG Pre-Group is defined in separate sections of this Terms of Reference.

The Bank's businesses and functions have documented business continuity plans to ensure continuity of critical operations functions in emergency situations and relevant drill exercises are conducted at least yearly. These plans have addressed interruptive situations caused by increasing environmental and climate changes. With remote computing technology and paperless workflow, the work-from-home readiness maintained at over 85% of our office staff since 2020. This enables our plans to be flexible and practical, and ultimately makes our operations more resilient.



#### Case study



The Major Incident Group ('MIG') continues to lead and monitor our contingency plans, and steers appropriate decision for crisis and emergency situations that the Bank faces. For example, during the start of the Fifth Wave of the pandemic in late January 2022, our MIG quickly responded to the lockdown of several buildings at Kwai Chung Estate, identified and provided supports to our staff who were impacted under the Government quarantine measures. Besides, trainings and simulation exercises were conducted for the MIG members to keep them abreast of the activation mechanism and on emerging threats like cyberattacks.

We have also deployed data analytic & visualisation tools to articulate the COVID-19 confirmed cases information, and the impacts to our operations. A map indicating the branches and business centres closed due to staff confirmed cases and a graph plotting the staff confirmed cases and trending were generated from the daily data to assist the MIG members to make informed decisions.

## ■ Being Proactive to Manage Risk ■ ■ ■ ■ ■

### Responsible value chain

Our financing decisions of the wholesale segment reflect our credit risk assessment, and the needs of our customers.

### Responsible financing

We have included environmental impact assessments in our standard credit evaluations. In the environmental impact assessments, we communicate with our customers to assess their environmental policies, achievements and risk mitigation measures.

We adopt [HSBC's sustainability risk policies](#) to assess sustainability risk when deciding whether to proceed with certain transactions. The sustainability risk policies cover agricultural commodities, chemicals, energy, forestry, mining and metals, thermal coal, UNESCO World Heritage Sites and Ramsar-designated wetlands.

These policies define our appetite for business in these sectors and seek to encourage customers to meet good international standards of practice. Where we identify activities that could cause material negative impacts, we will only provide finance if we can confirm clients are managing these risks responsibly. Such customers are subject to greater due diligence and generally require additional approval by sustainability risk specialists.

Our business units conduct sustainability risk analyses for all new and existing customers in sensitive sectors. This ensures that the products and services we offer are in line with [HSBC's sustainability risk policies](#). Corporate customers are reviewed regularly to monitor compliance with our policies. As of December 2022, we were fully compliant.

The workflows of labelling green / sustainability-linked trade finance facilities are in place to ensure the facilities we offer are comply with the international industry standards - Green Loan Principles and Sustainability Linked Loan Principles respectively.

For all approved green / sustainability-linked trade finance facilities, clients are required to obtain independent and external verification annually to ensure the facilities are aligned with GLP or SLLP respectively.

We observe the Equator Principles: voluntary guidelines for implementing sustainability standards in project finance. Currently, the Bank's portfolio does not have loan under the Equator Principles.



#### Case study

Based on the proxy voting guidelines, HSVM exercised over 97% of its voting authority to cast influence on its investee companies in 2022. This demonstrates the effort in ensuring the best interest of HSVM's clients.

HSVM became a Principles for Responsible Investment ('UNPRI') signatory in 2021. While the entity had implemented the responsible investment policy, in 2022, it further established the stewardship and engagement policy to govern its engagement practice including proxy voting to demonstrate its fiduciary responsibility to protect the interest of its clients. Proxy voting guideline explains the general principles and guidelines in detail that HSVM adopts in casting proxy votes and reflects the views of the investment team of HSVM.


## ■ Being Proactive to Manage Risk

### Supply chain integrity

We select and onboard new suppliers subjected to the minimum ESG requirements, related to environmental, social and governance matters.

We require our suppliers to comply with the Bank's supplier code of conduct before signing an agreement or submitting a proposal. In the revised version of the supplier code of conduct in 2022, the suppliers are required:

- ▶ to comply with the carbon emissions reduction goals
- ▶ to be a responsible consumer
- ▶ to respect as well as uphold human rights
- ▶ to be committed to diversity and inclusion
- ▶ to comply with our business conduct requirements
- ▶ to have an effective governance system in place to execute its compliance process

 >300

suppliers signed up to comply with the supplier code of conduct as of 31 December 2022.

↓ CO<sub>2</sub>

50% of our top 40 suppliers, i.e. half of our total spend, responded that they had committed in carbon reduction

More than 300 suppliers signed up to comply with the supplier code of conduct as of 31 December 2022.

The suppliers gain an understanding of the Bank's requirements in environmental, social and governance areas along the supply chain by reading the supplier code of conduct in the bidding documents and contract terms.

For financial products and services, we work with reputable third-party suppliers who have demonstrably high corporate standards. Rigorous assessments aim to help ensure any investment or insurance solution that we offer meets regulatory requirements and our own standards. We conduct regular reviews to ensure that service providers and their products meet the terms of our agreements.

95% of our active suppliers are from Hong Kong while the rest are from Asia, Europe and the United States.

We intend to adopt HSBC's mandatory policy to promote diversity and inclusion. It encourages sourcing from local, small and medium enterprises ('SME'), woman-led or ethnic-minority companies.

We have sent a questionnaire to our suppliers for understanding their carbon reduction plans. 50% of our top 40 suppliers, i.e. half of our total spend, responded that they had committed in carbon reduction.



### Human rights

To pledge our strong commitment to human rights, we reviewed the supplier code of conduct and updated the document in the fourth quarter of 2022.

In the revised supplier code of conduct, we emphasised on supporting, protecting and embracing human rights. Our suppliers need to comply with this Code before participating in a bidding activity or signing an agreement.

## ■ Being Proactive to Manage Risk

We do not have appetite to provide financial services to corporate customers in the agricultural commodities sector that are involved in, or are sourcing from, suppliers involved in the exploitation of people and communities, such as harmful or exploitative child labour or forced labour. Additional due diligence should be conducted in cases of mining and metal sector customers causing a severe adverse impact on human rights. In such events, we engage with the customer to consider the impact, the potential remedies, and whether we may have financed such an impact. For details, please refer to HSBC's [sustainability risk policies](#).

To strengthen our people-management capabilities and cultivate our inclusive culture, we provide training to our people managers. Regular workshops with case studies are available to combat workplace bullying and discrimination, embrace diversity. Upskilling workshops are also offered to people managers to be non-judgemental and empathetic to spot mental health issues and conduct appropriate conversation with team members in need. To support people managers in leading high-performing teams and provide best practices and advice on how to manage ambiguities and challenging situations when working virtually, a theme-based people management workshop teaches experienced managers to address on-the-job challenges.

5 incidents of discrimination, and no violation of the rights of indigenous peoples, were reported in 2022.

### Contractor Partnerships

We used a global online system for managing assessment and monitoring of third-party (supplier) risks and ensuring overall compliance of third-party management.

Inherent risks and residual risks are assessed, and related action are identified by the global online system.

There are measures to mitigate the contractual risks in phases: pre-engagement, contract negotiation and post-contract management. In addition, our line of businesses, legal, compliance and procurement Teams, as well as other subject matter experts participate in different phases of onboarding contractors. In the onboarding process, we have continuous communication and exchanges with the contractors, who are also required to sign the relevant contractual documents, e.g. non-disclosure agreement, letter of intent and contract, to align the understanding and commitment to the engagement.



### Online risk profiles

In 2023, we will adopt HSBC's mandatory policy to monitor the ESG compliance via the global online system. We can then keep track of whether the suppliers meet their commitments in carbon reduction and any other social, environment, governance requirements through the system.

At the same time, the procurement team will refer to a monthly risk report for mitigating risks.

