Governance

Being Proactive to Manage Risk

Risk Management Framework

Managing risk is a core part of our day-to-day activities. We protect our operations against compliance risks, and have strong, transparent corporate governance. Our risk governance forums hold regular meetings to ensure our governance and control framework is properly discharged, managed, sustained and communicated. Please refer to our Annual Report 2021 to learn more about our bank-wide approach to risk.

A minimum time commitment of 75 hours per annum for a Non-Executive Director ('NED') is set out in the letter of appointment which the NED would sign and acknowledge. Further, pursuant to the HKMA Guideline (Supervisory Policy Manual on Corporate Governance of Locally Incorporated Authorised Institutions ('CG-1')), the Bank's Directors are expected to attend all meetings of the Board and any Committees of which they act as Chairmen or members, especially where major issues are to be discussed.

Pursuant to the Conflicts of Interest Policy adopted by the Board, NEDs should consult the Bank's Chairman or the Company Secretary when they are considering whether to accept any additional or changed commitment. In deciding whether to permit the NED to take up the additional or changed commitment, factors including time commitment will be taken into account.

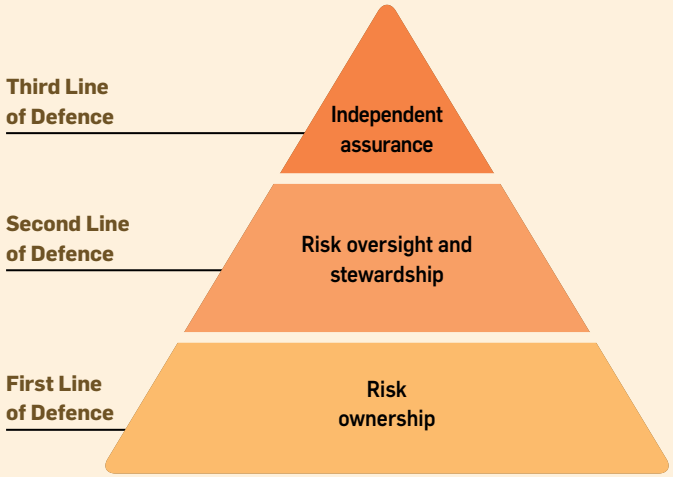
The Directors' attendance records have been set out in the Corporate Governance Report of the Annual Report 2021.

Governance

Being Proactive to Manage Risk

Three Lines of Defence Framework

We use three lines of defence to define roles and responsibilities within the Bank. The activity-based model delineates 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, and supports the delivery of conduct outcomes.



There must be a 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) to help support effective identification, assessment, management, and reporting of risks. It is our activities, not our job titles, which determine where we sit in the three lines of defence model.

Global functions may have responsibilities across both the first and second lines of defence, and therefore must segregate these responsibilities across 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.

The third line of defence, Internal Audit, 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.

Climate Risk Management Framework

We attach great importance to climate risk management. We established a climate risk management framework that is aligned with our parent company. We also developed a Climate Change Management Roadmap in 2021 with four focus areas: governance, strategy, risk management, and metrics and targets. We believe that a comprehensive risk management framework helps to identify and manage risks and enables us to make effective decisions and take appropriate risks as a result.

A Climate-related Risk Working Group at Risk function led by Chief Risk Officer (CRO) was formed in 2021 to oversee the climate related risk. The working group is comprised of subject matter experts and function heads of the Risk function. The working group is responsible for designing accountability for climate risk management and disclosure related to the Risk function for the Bank, update climate-related risk to ensure oversight by the senior management and oversee actions to mitigate climate-related risk to the Bank. Besides, our Risk and Finance functions work with relevant parties in resourcing, training, data and scenario analysis of climate risk with reference to the Bank's and our parent company's strategy. In addition, progress and issues for escalation relating to climate related risk are regularly updated at ESG Steering Committee and Risk Management Meeting to ensure senior management oversight. Besides, training sessions are organised for management and colleagues from time-to-time, for example, Climate Risk Programme Training was organised for the Bank's Executive Committee and Board members in September 2021.

Our Chief Executive and all Executive Committee members have incorporated ESG initiatives such as carbon reduction and/or sustainable finance with relevant KPI/ target in their 2021 performance objectives. Variable pay awards made to Chief Executive and other Executive Committee members have reflected the assessment of performance against scorecard objectives on both financial and non-financial objectives including risk performance and the ESG commitment in place.

Governance

Being Proactive to Manage Risk

Managing Different Types of Risk

ESG risk management

In accordance with the Hong Kong Exchanges and Clearing Limited ('HKEx')'s ESG Guide, the Board determines and evaluates the ESG risks that we face. It ensures that effective risk management and internal controls are in place. Reviews of these systems were conducted and attested by the management. Management presented its confirmation on the effectiveness and adequacy of the Bank's disclosure framework, including risk management and internal control systems relating to Environment, Social and Governance, to the Board in April 2021.

The Bank formulated its ESG strategies, raised staff awareness of the importance of and issues relating to ESG, assisted customers with migration to low-carbon journey, and strengthened ESG disclosure to align with latest regulatory requirements. The Board approved the Bank's 2021 ESG Strategy and Implementation Plan, as reviewed by the ESG Steering Committee and Executive Committee ('EXCO'). The Plan mainly focused on satisfying key stakeholders' expectations on relevant ESG topics, and prioritising areas for investment based on the Bank's strength and Strategic Plan.

The target outcome of the 2021 ESG Strategy was to make the Bank a leading entity to drive ESG in the banking industry, from stakeholders' perspective (which included the staff and customers of the Bank, as well as the community, regulators and analysts).

To achieve such strategy, three key focuses, six key pillars and three key messages were developed in the 2021 ESG Implementation Plan. The Board has overall responsibility for ESG matters identified by EXCO based on the recommendation of the ESG Steering Committee, and the integration of such matters into the Bank's strategies. ESG updates would be provided to the Board at least twice a year. Meanwhile, ESG performance of the Bank and the relevant key performance indicators would be measured, monitored and reported on a regular basis. The Bank has committed to achieve "Carbon Neutral" in its operations by 2030.

Our Chief Risk Officer (CRO) represents the risk team on the ESG Steering Committee and leads the incorporation of climate risk into our risk management.

Compliance

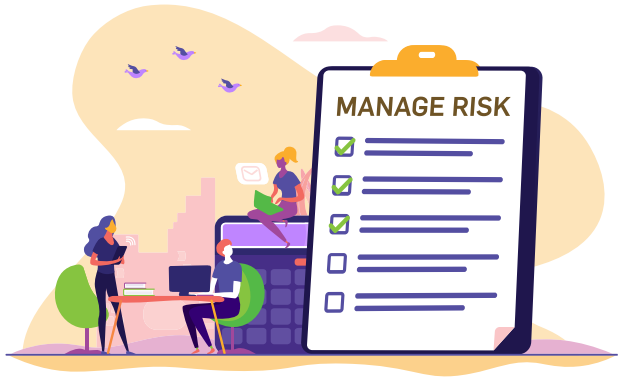
Our credibility relies on our operational integrity and the transparency of the information we provide to stakeholders. Upholding strong corporate governance, adherence to the highest ethical standards and effective risk management are essential to being an accountable, transparent and well-managed company. Compliance issues are discussed and reviewed by the Board and management committees. 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 quality, professionalism and integrity throughout our business. Internal controls, risk management, compliance, and legal and regulatory requirements are considered at Board meetings.

In 2021, all directors and staff undertook various training on values and conduct. This covered, among other topics, whistleblowing, anti-bribery and corruption. Such training is further provided from time to time to our directors and senior leaders. We require all our staff members to comply with relevant codes of conduct. For details, please refer to the "Staff code of conduct and staff awareness" section.

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

The Audit Committee reviews our financial reporting, the nature and scope of audit reviews, and the effectiveness of our control and compliance relating to financial reporting.

No non-compliance with laws and regulations that resulted in significant fines or non-monetary sanctions was recorded in 2021.



Governance

Being Proactive to Manage Risk

Financial and tax risks

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

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.

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 are committed to complying with the spirit and the letter of the tax law in all territories and countries in which we operate and maintaining an open and transparent relationship with tax authorities. Relevant financial information is disclosed in our Annual Report.

We follow our parent company's tax policies, principles and strategies.

Competition

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

In 2021, no judgements were entered against Hang Seng for breaching the Competition Ordinance.

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 continue to invest in expertise, partnerships and systems.

We are committed to high ethical standards. Our policies on anti-money laundering, sanctions, and anti-bribery & corruption aim to ensure that risks identified by the bank are appropriately mitigated.

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

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

The global fraud landscape is characterised by increasingly sophisticated attacks targeting online banking and other digital services. Under our multi-year fraud transformation programme, launched in 2018, we are investing in training our people, as well as enhancing our technology-based defences.

We are constantly striving to improve the way we detect and prevent financial crime and explore technologies that help us build on existing capabilities. Fighting financial crime is a key area that can benefit from innovation and we're 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 staff to report suspected fraud and forgery, protecting our customers from suffering financial loss.

We uphold the standards that the Bank consistently operates ethically, honestly and with full accountability. We ensure that our 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 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 also receive additional, specialised learning regarding the detection and deterrence of financial crime.

In 2021, staff in Hong Kong received over 93,836 hours of policy and procedural learning on bribery and corruption, money laundering and sanctions, conduct, values and regulations

Governance

Being Proactive to Manage Risk

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

In 2021, no judgements were entered against Hang Seng for failing to fight financial crime.

Anti-bribery and corruption

We have adopted a three-year programme to advance the Bank's anti-bribery and corruption risk management capability. We have strengthened our controls and processes, and improved our global register for Associated Persons. The programme now focuses 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 operate a zero tolerance approach to bribery and corruption and considers such activity to be unethical and contrary to good corporate governance. The Bank, its staff and associated persons are prohibited from engaging in bribery and corruption.

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.

Anti-corruption training are mandatory for **all** staff in Hong Kong including contractors.

Anti-corruption training hours delivered to Directors in 2021: **11 hours**

Percentage of Directors received anti-corruption training in 2021: **100%**

Data privacy

We continually strengthen our data privacy policy, instruct staff to report security incidents and provide 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 customer data are set out in an internal procedure manual. Our clear desk policy reduces 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. Our legal function and Data Protection Officer provide second-line oversight. Officers at functional and business units promote data protection and disseminate information on guidelines and developments (refer to Customer Privacy in Our Customers).

Data privacy principles are set out to manage data privacy risk. Four mandatory controls are implemented 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 identifiable data, and keeps evidence of the process, to make sure the Bank can demonstrate that it complies with data privacy laws.

- Privacy Impact Assessments:

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

- Internal and External Data Transfers:

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

- 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 laws. These disclosures are usually made in response to external requests.

Governance

Being Proactive to Manage Risk

As of the end of 2021, Wealth and Personal Banking ('WPB') existing customers opt-in rate for customer data used for secondary purposes, e.g. marketing (non-private banking customers) was 59.8%. Meanwhile, the marketing opt-in rate for the Bank's commercial banking customers was 90.4%.

Source	Customer privacy upheld* complaints
Outside parties	1
Regulatory bodies	0
Total	**1**

Type	Customer privacy upheld* complaints
Identified leaks	1
Thefts	0
Losses of customer data	0
Others	0
Total	**1**

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

Cybersecurity

The cyber threat landscape continues to evolve at a fast pace, leveraging the ubiquitous nature of, and dependence upon technology. Driven by the rapid advancement of technology, controls designed to effectively mitigate cybersecurity risk will become outdated, circumvented or obsolete over time, as malicious threat actors continue to enhance their methods of attack. Our regulators, customers and clients expect us to take the necessary steps to protect the markets, their data and business interests to the best standards available in the industry. We have invested over the last few years to attain standards of good practice in cybersecurity and is committed to maintaining this position in the future. Not to do so could result in loss of customer and client trust and regulatory confidence, leading in turn to loss of market value, customer attrition, and regulatory censure.

To maintain these standards of good practice, due to the dynamic nature of the threat environment, we need to continuously review the cyber risk appetite and the ongoing effectiveness of our controls in mitigating these risks. While in most cases it is extremely difficult to reduce the potential impact of a cyberattack, it is possible, through ongoing control investment, to reduce the overall likelihood of a cyber risk being realised. This means that our controls require continuous review and augmentation and that an end state to cyber control effectiveness and less than high residual risk is likely unachievable. Cybersecurity risk, is likely therefore to remain residually high at a Group-wide level for the foreseeable future. To ensure this position does not degrade over time, a continued re-evaluation of effectiveness and where necessary investment in control maintenance and enhancement does however, enable organisations like us to keep residual risk at an acceptable level over time.

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

Banks are high-profile targets for criminals seeking financial gain, personal information and disruption. The potential effects of cyberattacks include financial loss, reputational damage and loss of customers.

Protecting our customers and our company from such threats is a key component of our strategy to become a global, connected, digital business. All our IT infrastructure in our operations adopt the industry-standard National Institute of Standards and Technology ('NIST') framework. We engage an external consultant to conduct an annual cyber resilience assessment with this framework to assure the security of our IT infrastructure and identifies areas that require improvement and funding.

To strengthen our capability, we have developed a Cybersecurity Maturity Improvement Programme. Using threat scenarios witnessed in our industry, our cyber risk quantification model calculates the likelihood of an attack being successful. This determines the value of projects aimed at risk reduction.

Governance

Being Proactive to Manage Risk

To support the Board and senior management's oversight of cybersecurity, we regularly report on our strategic programmes and key indicators. Our cybersecurity strategy is reviewed and business risk profiles, mitigation awareness, internal and external cybersecurity incidents, and regulatory requirements are discussed.

We offer security training to all users such as executives and their assistants, privilege users, IT end users, software developers, third-party service providers and adopt automated cybersecurity assessment tools. Vulnerabilities across the network, operating systems, application layer, and in-house custom software are managed on a centralised platform and remediated according to priority.

Meanwhile, we continue to invest in defence against ever more sophisticated cyberattacks. We have enhanced our event detection, incident responses, secure development, vulnerability remediation, and protection against malware, application layer attacks and data leakage. Also we have strengthened our third-party management by including cybersecurity due diligence which delivers stricter governance and enforced third-party security testing prior to contract approval.

Staff are required to report cybersecurity incidents to our 24/7 hotline as soon as possible once discovered. Such incidents include the loss of restricted information, leakage of customer data, and suspected or confirmed cyberattacks. These are then dealt with by our cybersecurity analyst and Security Operations Centre, and are reported to management for direction on remediation. Cybersecurity incident response procedures have been established and are tested regularly to enhance the level of understanding in terms of roles, protocols, internal communication paths and escalation procedures across the business in the event of a cybersecurity incident.

We also share intelligence with law enforcement and the industry. This improves our understanding of, and ability to respond to the evolving threats faced by our industry.

Cybersecurity learning was delivered throughout 2021. It covered data security, email security and phishing, password management, access control, incident reporting and escalation, secure use of communication devices and social media, our clear desk policy, information classification and labelling, system vulnerabilities and patching, ransomware and deliberate denials of service.

Periodical cyberattack drills are conducted to enhance the level of understanding in terms of 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.

Number of data breaches in 2021, including those involving personally identifiable information (PII): 0

Training or communication regarding cybersecurity offered in 2021 included:

- Mandatory e-learning for all staff
- Briefings to the Board and Executive Committee members
- Role specific training for staff who have access to consumer and commercial credit data
- Seminars hosted by senior leaders which also featured expert speakers
- Cybersecurity awareness and training regarding data security has been delivered to all staff including selected user groups and the security community on a regular or as-needed basis
- Training delivered to selected user group and the security community such as executive assistants and privileged access users on a risk and skill-based basis

Governance

Being Proactive to Manage Risk

Equal opportunities, non-discrimination and human rights

Human rights matters are complex and the roles and responsibilities of business and other stakeholders are subject to ongoing international dialogue. We are open to engaging in this dialogue.

We are committed to 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 advance based on merit. We uphold diversity and inclusion when hiring. Recruitment is merit-based and free from bias and discrimination.

To nurture an inclusive and speak-up culture, all staff undertook mandatory training on values and conduct. Workshops are organised for people managers to equip them with knowledge and skills to handle discrimination, harassment and bullying. Diversity learning is also embedded in the induction programme for new joiners.

We have Disciplinary Procedures for Misconduct and Gross Misconduct Policy setting out principles which should be adhered to when dealing with disciplinary matters to ensure that fair, non-discriminatory and consistent methods are used. To ensure consistent approach and high standard on managing misconduct and inappropriate behaviours, guidance materials is available to managers for determining disciplinary sanction and performance and reward outcomes.

The Management Accountability Framework is also in place, outlining the expectations for managers and holding them accountable for their role in protecting the Bank from conduct and regulatory breaches.

Aligning with values of our parent company, we value difference, champion inclusivity and foster a respectful workplace free from discrimination, or violation of human rights. The Bank's Staff Code of Conduct outlines our expectations on human rights matters. With Board representatives' involvement, the People Committee reviews the Staff Code of Conduct on an annual basis and as when required to reflect the latest regulatory requirements and the Bank's internal policies.

Our commitment to human rights extends to our value chain (refer to Protecting human rights). No incidents of discrimination, or violation of the rights of indigenous people, were reported in 2021.

Staff code of conduct and staff awareness

The Staff Code of Conduct is uploaded to our employee self-help portal in English and Chinese. By issue of circular, all employees and contractors are informed of any changes of Staff Code of Conduct and are reminded to read and abide by the rules and regulations. All employees and contractors are required to complete an online curriculum for the Code to ensure their understanding on the rules and regulations set out in the Code.

With Board representatives' involvement, the People Committee reviews the Staff Code of Conduct on an annual basis and as when required to reflect the latest regulatory requirements and the Bank's internal policies.

In 2021, we launched the e-learning programme "Guide to the Code of Conduct" to all staff, aiming to help our staff better understand the expected behaviours, apply the requirements of the Code to everyday environment and clarify questions that they may have.

In 2021, there was one identified material case of non-adherence to our Staff Code of Conduct. Apart from reporting to relevant regulator(s) where appropriate, the Bank has been proactive in taking consequence management, depending on the severity level of the cases.

Governance

Being Proactive to Manage Risk

Conflict 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 in sensitive or high-risk areas are required to adhere to specific rules and undergo training on how to avoid conflicts of interest.

Whistleblowing

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

Our internal whistleblowing portal is a process to promote consistency in controls, investigation, reporting, oversight, and governance of all whistleblowing activities. With our internal whistleblowing portal, which is accessible through 24/7 hotlines and online portal in multiple languages managed by independent third party, employees can raise concerns confidentially while employees may 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 subject matter experts, in accordance with our parent company's policies and standards.

A well-established employee grievance procedure is in place and best endeavours are made to ensure investigations are carried out objectively in light of the information provided and resulting actions are taken. In 2021, 9 grievance cases were reported to HR through HR online portal. No consequence management actions were taken as no cases were identified as upheld, while 1 case is not actionable and 1 case is still under investigation.

To regularly monitor and assess the Bank's culture, the Bank reviews the Bank's Culture Statement annually and conducts an internal assessment "Culture Dashboard" every six months, to assess the strength of the Bank's culture in enabling the fulfilment of our purpose to support customers and communities; protect the Bank and its investors; and uphold both the standards expected by regulators and integrity of the financial systems within which we operate. Culture is assessed through:

- Employee sentiments – how people feel about our culture, measure by the employee survey
- Behaviours – What people see around them, measure by the employee survey
- Business Outcomes – How people's behaviours impact business outcomes and customer experience, measure by personal conduct cases, compliance breaches, financial crime activity, whistleblowing, incentives and recognition, customer centricity and customer experience

Analysing the relationship between how people feel about our culture, how they behave, and whether or not this is seen to play through into business outcomes enables identification of areas of strengths and weaknesses while informing where remediation efforts should be directed.

Suppliers are encouraged to immediately report to us by email in the event of concerns about ethical conduct, including bribery and corruption. Upon receipt of such reports, an independent team investigates and proposes follow-up actions. We also expect suppliers to have grievance mechanisms in place. Our parent company's Ethical and Environmental Code of Conduct for Suppliers of Goods and Services provides clear guidance on grievances and disciplinary practices, and includes provisions prohibiting mental, physical and verbal abuse.

At times individuals may not feel comfortable speaking up through the usual channels. Our global whistleblowing channel allows our colleagues and other stakeholders to raise concerns confidentially, and if preferred, anonymously (subject to local laws). Enhancements to the channel in December 2020 mean the majority of concerns are now raised through an independent third party offering 24/7 hotlines and a web portal in multiple languages.

In 2021, there were 27 cases of whistleblowing cases and 14 of them were investigated and closed. The rest of the cases were still under investigation or review as of 31 December 2021. Out of the total 27 cases of whistleblowing cases reported, 100% of the cases was reported through confidential whistleblowing platform.

Governance

Being Proactive to Manage Risk

Business continuity planning

Business continuity and incident management policies are formulated with reference to the our parent company'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 learned from 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 consists of senior management representatives and is chaired by the Chief Operating Officer to provide guidance and to ensure governance of the Bank's business continuity management four times a year.

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.

With remote computing technology and paperless workflow, the work-from-home readiness maintained at over 85% of our office staff since last year.

This enables our plans to be flexible and practical, and ultimately makes our operations more resilient.

The Major Incident Group continues to lead and monitor our contingency plans, and steers appropriate decision for crisis and emergency situations that the Bank faces.

Responsible Value Chain

Our financing decisions reflect our principles, our risk assessments, and the needs of our customers.

Responsible financing

Our corporate lending policy details our requirements regarding sustainability risks.

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.

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 our sustainability risk policies. Corporate customers are reviewed regularly to monitor compliance with our policies. As of December 2021, we were fully compliant.

We send updates on environmental or social risk-related policies to all relevant staff on a timely basis. Up-to-date policies and guidelines can be accessed by relevant staff via the intranet. Training on our environmental and social policies is included in the New Joiners Induction Programme.

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.

For customers within the scope of our sustainability risk policies, we assess the potential impact of their business on people and the environment, and their ability to manage that impact. Then, we allocate a sustainability risk rating to each of these customers. Specific standards apply in high-risk areas and, where applicable, approvers take sustainability into account when recommending a relationship or transaction. They also ensure that the sustainability risk ratings are correct, and suggest amendments where necessary.

Governance

Being Proactive to Manage Risk

Responsible Financing

We carefully assess environmental and social risks when deciding whether to make a loan or investment. We also adopt our parent company's sustainability risk policies. Specific guidelines apply to businesses in sensitive sectors, including those outlined on the right. These guidelines are refined and updated as required and we have mechanisms to ensure our customers remain compliant with these policies.

This embeds ESG into our investment approach, product design and day-to-day operations.

Agricultural commodities

We undertake special assessments of customers involved with palm oil, soy, cattle ranching or rubberwood sectors. Enhanced governance aims to ensure that we maintain relationships only with customers who engage in sustainable development. They must operate in accordance with international standards and industry practice, and provide a public commitment to do so.

Energy

We avoid financing new projects involved in thermal coal-fired power plants, offshore oil or gas projects in the Arctic, greenfield oil sands projects, large dams for hydro-electric projects inconsistent with the World Commission on Dams Framework, and nuclear projects inconsistent with the International Atomic Energy Agency ('IAEA') standards.

World Heritage Sites and Ramsar wetlands*

We avoid supporting projects that may have unacceptable impacts on sites of special international significance.

Forestry

We work with customers to promote sustainable forestry.

Chemicals

We adhere to national and international standards. We communicate with our customers to achieve sustainable chemical manufacturing.

Defence equipment

We are restricted to provide financial services to customers who manufacture, sell, purchase or use anti-personnel mines and cluster bombs and other weapons as per the guidance.

Mining and metals

We assess potential customers linked to human rights abuses, and those with poor track records for work-related fatalities and accidents. We avoid financing for thermal coal mines, mines using mountaintop removal ('MTR') or customers dependent on MTR in the Central Appalachian Mountains of the United States of America, or customers commencing the disposal of tailings in rivers or shallow sea-water in or since 2007.

* Remark: The Convention on Wetlands is an inter-governmental treaty to protect wetlands of international importance, signed at Ramsar in Iran in 1971.

Governance

Being Proactive to Manage Risk

Responsible investment

Based on the Proxy Voting guidelines, Hang Seng Investment Management Limited ('HSVM') has exercised over 99% of its voting authority to cast influence on its investee companies in 2021. This demonstrates the effort in ensuring the best interest of HSVM's clients.

HSVM has also established the Responsible Investment policy to further integrate responsible investment concept into the day-to-day management of its investments and clients' portfolios.

HSVM became a Principles for Responsible Investment ('UNPRI') signatory in December 2021.

Supply chain integrity

We rely on vendors, agencies and third-party financial product suppliers to support our business. This enables us to offer diverse products and services, but potentially exposes us to risks, both reputational and otherwise.

Effective supply chain management is therefore vital to safeguard our brand and business, and to promote responsible practices among companies in our community. We require contractors and suppliers to adhere to our stringent environmental, social and ethical standards and to the principle of continual improvement.

We maintain transparency and fairness in our procurement and contracts processes. Procurement is done on a competitive basis, and strict procedures govern employee conduct when handling such processes. Employees are trained to understand our internal controls and monitoring requirements.

Our third-party risk policy provides clear details of the standards we expect our suppliers to uphold, and how we assess their performance via supplier's self-assessment on commitment to reducing carbon emissions and adding ESG element into tender scorecard. As of 2021, we had 1,684 contracted suppliers. All are required to acknowledge their compliance with the our parent company's Ethical and Environmental Code of Conduct for Suppliers of Goods and Services before contract award. Relevant records will be kept in online platform by our global utility team. This code communicates our economic, environmental and social standards, and the requirement for a governance and management structure that ensures compliance.

We monitor suppliers following their appointment and reserve the right to review their policies on demand, procedures or documentation. We may also request an on-site audit to assess compliance with ESG and local regulations.

To ensure that suppliers clearly understand our requirements, sustainability standards are included in our purchasing policy documentation. This enables suppliers to assess their status and develop a plan that meets our standards. They must also make reasonable efforts to ensure that their own supply chains are aware of, and comply with, our standards. We require our suppliers to establish environmental management system, as part of the due diligence process. To support our carbon-neutral ambition, we also assess the relevant commitment and performance of our suppliers, and ensure environmental considerations are incorporated in their purchasing process.

For financial products and services, we work with reputable third-party suppliers who have demonstrably high corporate standards. Rigorous assessments 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.

Electronic signatures in our procurement process help reduce paper consumption and lead times, and provide us with enhanced supplier and information management controls. We encourage and assess suppliers and contractors to use and offer environmentally friendly and recycled products wherever possible.

Using local suppliers demonstrates our support for our community, while eliminating unnecessary transportation reduces our impact on the environment. According to our payment records in 2021, around 90.4% of our suppliers have presences in Hong Kong. The remainder are in Asia, Europe and the United States.

Governance

Being Proactive to Manage Risk

Human rights

Protecting human rights

Our commitment to human rights extends to our value chain. Our sustainability standards require suppliers to commit to respecting the rights of their employees and of individuals in their communities, and to complying with all relevant legislation, regulations and directives in the countries and areas in which they operate.

We avoid associating with entities with a high risk of human rights violations. Our parent company's Ethical and Environmental Code of Conduct for Suppliers of Goods and Services prohibits suppliers who restrict freedom of association or rights to join labour unions or who use child or forced labour.

We require our suppliers' employment practices should observe our parent company's requirements, including the principles of the Universal Declaration of Human Rights, the International Labour Organization Declaration on Fundamental Principles and Rights at Work, the OECD Guidelines for Multinational Enterprises, the Codes of Practice on Employment promulgated by the Equal Opportunities Commission in Hong Kong and local regulations.

Our expectations regarding human rights are communicated to our suppliers via their acceptance of the Ethical and Environmental Code of Conduct for Suppliers of Goods and Services. They must state compliance with this code by signing and returning it to us before the contract award stage.

They must:

- Respect the rights of the people and communities in which they operate, and strive to improve the lives of those people and the conditions in those communities
- Not use child, underage and forced labour
- Not engage in or support human trafficking
- Provide evidence of due diligence regarding their supply chain and labour processes, to ensure they comply with laws on slavery and human trafficking

We assess clients before we commit to corporate lending. We do not provide financial services to customers in the agricultural commodities sector that are involved in, or sourcing from, suppliers involved in the exploitation of people and communities, such as child labour or forced labour. We analyse incidents including mining and metal sector customers causing severe adverse impacts on human rights. In such events, we engage the customer and consider the impacts, the potential remedies, and whether we should continue the relationship. For details, please refer to our sustainability risk policies.

Contractor partnerships

For all operating and capital expenditure, our procurement policy strives for efficiency, transparency, segregation of duties and the most suitable buys. Our procurement team engages with as many suppliers as possible and briefs bidders on our tender requirements. We apply fair competition principles to all applications from appropriately qualified parties, and consider every proposal in an unbiased and honest way. We have zero tolerance for corruption and bribery.

We meet with existing and potential suppliers to review and strengthen business relationships, and keep abreast of market trends.

Before order release and payment, suppliers are subject to checks and ongoing screening. These ensure they do not reside in, are not incorporated in, and do not maintain their primary business operations in sanctioned countries, nor are named on global sanction lists.

Online risk profiles

Our online platform enables internal users to assess service and supplier risks relating to:

- Bribery and corruption
- Money laundering and sanctions
- Business continuity and incident management
- Accounting
- Regulatory compliance
- Security of people and physical assets
- Subcontracting
- Tax
- Insurable risk
- Information and cybersecurity risks

The platform helps us in monitoring risks and supplier management. It automatically proposes and tracks the completion of related controls. It ensures compliance with our third-party risk management policy. And it enables on-demand reporting, which greatly enhances visibility and control of the most important risks and services. This helps satisfy growing demands from regulators for supplier risk management.

In 2021, there was no confirmed incident when contracts with business partners were terminated or not renewed due to violations related to corruption.