Chapter 4 – Risk Management and Internal Controls

- Risk management and internal controls are important safeguards that enable an issuer to achieve its operational, reporting and compliance objectives. There is, however, no "one-size-fits-all" approach in terms of putting in place and maintaining an effective system of risk management and internal controls - each issuer has to first identify its strategic objectives, consider relevant risks to achieving these objectives and then create a system that is appropriate for the issuer's individual risk profile and circumstances.

- As an issuer's business, and its risk profile, may change over time, it should monitor its risk management and internal control systems on an ongoing basis and conduct periodic reviews of the systems' effectiveness.

Roles and responsibilities

Role of the Board

1. Under the Listing Rules, the board is ultimately responsible for the issuer's risk management and internal controls[73]. Effective risk management and internal controls start with the board setting the appropriate "tone from the top" and instilling a commitment to compliance and ethics in the issuer's culture and operations.

2. The board should set clear objectives for the issuer, identify existing and emerging risks for such objectives and determine the level of risks it is willing to accept in the course of pursuing the issuer's objectives. Based on this analysis and the issuer's risk tolerance, the board can then work with the issuer's management on the establishment and maintenance of appropriate and effective risk management and internal control systems. In addition, the board should ensure that its approach to risk tolerance has been properly communicated throughout the organization.

3. While the board may delegate certain aspects of its work to management and relevant departments (e.g. internal audit) or external providers (e.g. internal control consultants), proper oversight over the design, implementation and operational effectiveness of the risk management and internal control systems is ultimately the board's responsibility.

4. The board should monitor the issuer's risk management and internal control systems on an ongoing basis. A review of the systems' effectiveness should be conducted at least annually[74]. For each reporting period, the board should provide a statement in the corporate governance report that acknowledges its responsibility for the issuer's risk

[73] MDR paragraph H(a) and Principle D.2.
[74] MDR paragraph H.

management and internal control systems and confirms that these systems remain appropriate and effective[75].

Role of the Management

5. While the board takes the lead in establishing the issuer's risk management and internal controls systems, it is the responsibility of the management to design and implement that system and ensure it is operating effectively on a day-to-day basis[76]. To facilitate the board's oversight, the management should provide the board with relevant information and periodic confirmation as to the implementation and effectiveness of risk management and internal control systems.

6. Management's role includes designing and implementing an appropriate framework for the systems consisting of relevant policies and procedures; and the appropriate delegation of roles, responsibilities and authority among the issuer's departments and staff (and involved external providers).

7. The framework should include appropriate structures and procedures for the ongoing monitoring and regular review of the operational effectiveness of risk management and internal control systems. The management should provide regular reports to the board on progress and timely updates on any issues identified so that the board can exercise its own supervision and oversight.

Role of the Audit Committee

8. The audit committee shares responsibility for the oversight of the issuer's risk management and internal control systems (unless such oversight is expressly allocated to another board committee (e.g. risk committee)) [77].

9. The audit committee should seek discussions with management to ensure the existing internal control systems remain appropriate and effective. The audit committee should also consider major findings on risk management and internal control matters and management's response to these findings. The audit committee should ensure that it reports its findings to the board from time to time and elevates any concerns for the whole board's consideration as appropriate.

10. The board should ensure that the audit committee has sufficient resources and is provided with relevant and timely information to perform its duties in relation to the oversight of the issuer's risk management and internal control systems.

[75] MDR paragraph H(a).
[76] Principle D.2.
[77] CP D.3.3(f).

Risk management

Risk identification and assessment

11. An issuer's risk management closely interacts with the operational, reporting and compliance objectives of the issuer and the issuer's framework of internal controls. To understand its exposure to risks, an issuer should first define clear objectives:

- **Operational Objectives:** Objectives that facilitate effective and efficient operations by enabling the issuer to achieve strategic, operational and financial performance goals and safeguard such goals against business, operational, financial, compliance and other risks (including fraud).
- **Reporting Objectives:** Objectives that safeguard the quality of the issuer's internal and external reporting, including through the maintenance of proper records and processes that generate timely, relevant and reliable information.
- **Compliance Objectives:** Objectives that focus on the issuer achieving regulatory compliance (and compliance with applicable laws) and adherence to internal policies with respect to the operation of the issuer's business.

12. After defining its objectives, an issuer can identify the risks that may impact or prevent it from achieving these objectives. The risks that each issuer encounters will be different, depending (among other things) on the scale, complexity and geographical locations of its business operations. An issuer should undertake the following steps:

(1) **Analyse the source of potential risks**

The scope of the issuer's analysis should be broad and cover risks that can develop from internal processes and infrastructure (for example IT infrastructure, issuer's resources, assets, organisation and operational infrastructure), as well as from external interactions, developments and threats (for example political or economic environment, business developments, and interaction with outside parties). Without limitation, the scope for analysing potential risks should be wide enough to cover material ESG risks, cyber security risks, and fraud risk.

(2) **Evaluate and prioritise the identified risks**

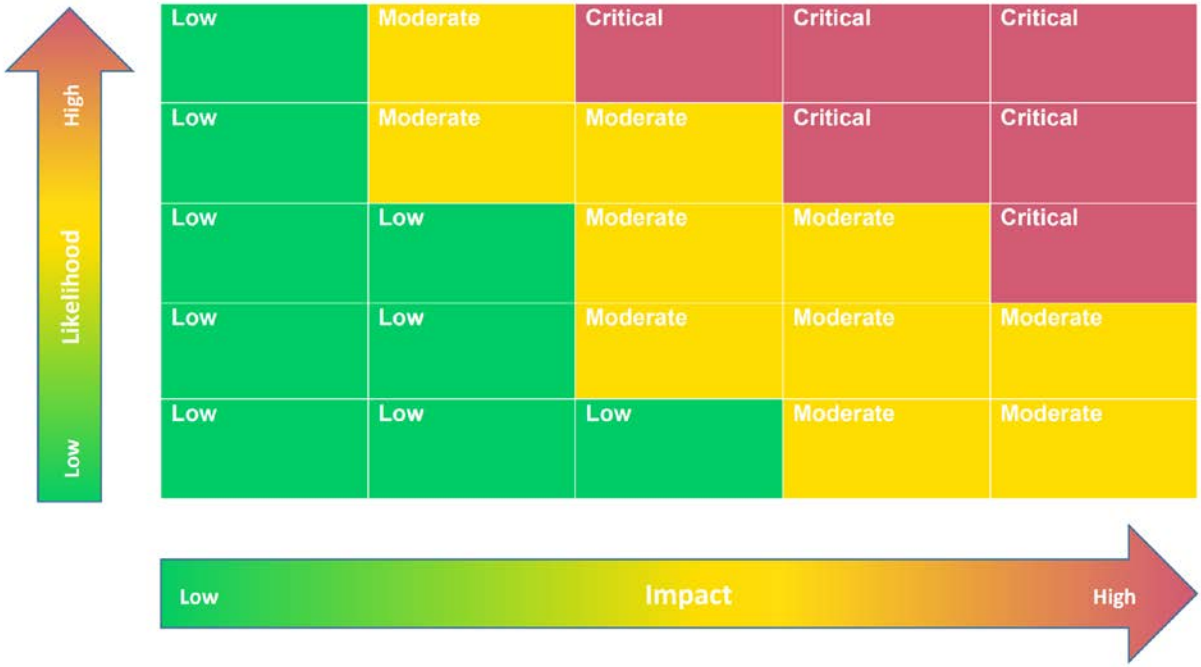
To formulate its risk management strategy, the issuer will have to evaluate identified risks and develop procedures to prioritise addressing significant risks and allocate relevant resources accordingly. This evaluation should be conducted by the board with the support of the issuer's management.

(3) **Monitor existing risks (and the emergence of new risks)**

The issuer should constantly monitor the development of current and emerging risks. For the purpose of tracking risks and logging risk responses, an issuer may consider creating a risk register of all identified risks with a particular focus on significant risks. This risk register should be updated regularly and, in any event, at least annually.

Risk heat map

13. The issuer may make use of a "risk heat map", as illustrated in the diagram below, to assess the impact of the identified risks that are recorded on its risk register. In the "risk heat map", the issuer's top risks (which may include existing and potential risks) should be plotted into a matrix and graded in accordance with their likelihood of occurrence and impact on the issuer's objectives and goals. The board can consider the resulting "heat" rating and review / adjust the risk management and internal control systems to mitigate such risks.



Practical considerations for boards

Questions the board should ask when considering the issuer's procedures to identify and assess risk:

- Has the board considered and formulated clear objectives? Is the issuer's process of risk identification and assessment focused on safeguarding these objectives?
- Is the current risk identification procedure wide enough to cover not only existing risks but also emerging risks? Is there a robust process of continued monitoring for new / emerging risks (and re-evaluation of existing risks)?
- What is the level of the issuer's risk tolerance in pursuing its objectives? Has this been clearly communicated throughout the organisation?
- Has the risk assessment sufficiently taken account of the impact of each risk on the issuer's objectives? Are the risk management strategies aligned with the issuer's risk tolerance?
- Are there any procedures for regularly adjusting the existing risk assessment to reflect developments or changes in the issuer's objectives or risk profile?
- Have sufficient resources been committed to the process of risk identification and assessment?
- Do channels exist for different functions within the issuer to elevate risks or voice concerns in terms of the existing risk assessment procedures?

Internal controls

Components of risk management and internal control systems

14. While there is no "one-size-fits-all" approach to designing an effective and appropriate system of risk management and internal controls, international bodies have developed a framework setting out components that should be covered by an issuer's internal controls. When designing their risk management and internal control systems, issuers can consider and apply these components in accordance with their unique risk profile and circumstances.

Table 6: Components of risk management and internal control systems[78]

Components	Principles
Component 1 - Corporate culture / control environment This refers to the issuer's overall culture of internal controls, i.e. the issuer's control environment. It is important that, throughout the various levels of the issuer's operation and staff, there is a commitment to integrity, compliance and ethical behaviour. This commitment starts at the board level as the right "tone from the top" is required to achieve buy-in across the organization.	1. **Integrity and Ethical Values** – There is a firm commitment to ethical standards and culture of integrity, including through appropriate policies and procedures (whistleblowing policy, code of conduct, etc.). 2. **Independent Board Oversight** – The board maintains independence from management and exercises appropriate oversight of the internal control system's implementation (among others, through the audit committee). 3. **Organizational Structure** – There is a defined structure of authority and responsibility to implement operational, reporting, compliance, and business objectives. 4. **Human Resources** – Staff recruitment, development and retention is focused on alignment with the issuer's objectives, in particular in terms of culture, integrity and compliance. 5. **Accountability** – There is a system of responsibility and accountability in place that includes regular reviews of staff performance including on compliance metrics related to the internal control systems.
Component 2 - Risk assessment This refers to ongoing risk assessment across all aspects of the issuer's business. An issuer needs to operate with clear objectives which allow for an ongoing analysis of risks (including fraud risk) to such objectives – this includes identifying and analysing significant change to (among other things) ensure internal controls remain effective.	6. **Identification of Objectives** – Establish strategic operational, reporting, and compliance objectives to allow for the identification of potential risks and the impact of such risks to the objectives. 7. **Identification of Risks** – Conduct assessment of risks for the issuer's objectives and adopt plans for risk management. 8. **Fraud Risks** – Consider fraud risks and adopt appropriate steps to manage such risks. 9. **Impact on Internal Controls** – Consider the impact of its risk assessment on its internal control systems and make any changes as required.

[78] Source: The Internal Control—Integrated Framework (ICIF-2013) published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) formed by five global accountancy and auditing organizations. See also the Hong Kong Institute of Certified Public Accountants, Technical Bulletin, Assistance Options to New Applicants and Sponsors in connection with Due Diligence Obligations, including Internal Controls over Financial Reporting.

Component 3 - Internal controls This describes the internal control systems / control activities put in place to respond to the risk assessment and mitigate the identified risks. This includes activities, processes, policies and communications required to establish a strong framework of internal controls and respond adequately to risks.	10. **Internal Controls** – The issuer adopts and implements a system of internal controls (or control activities) to manage and mitigate risks. 11. **Technology** – The internal control systems include appropriate controls over technology / IT and online infrastructure / the use of AI. 12. **Policies / Procedures** – The internal control system is supported by appropriate policies and procedures.
Component 4 - Information and communication This requires an issuer to put in place procedures to ensure that the internal control systems are supported by appropriate and up-to-date information and data, and, for such information to be adequately communicated internally and externally (as applicable).	13. **Information and Data** – To ensure proper operation of the risk assessment and internal control systems, the issuer deploys accurate, timely, and sufficiently detailed information and/or data (issuers should also critically assess the impact of the use of AI on such processes). 14. **Internal Communication** – Relevant information is communicated in a timely and thorough manner to support the effective operation of the internal control systems. 15. **External Communication** – Communication designed to support the effective operation of internal control systems should also involve external stakeholders (as required).
Component 5 - Monitoring This requires an issuer to continuously monitor the internal control systems and ensure that they remain fit for purpose, and that potential deficiencies are communicated in a timely manner such that appropriate actions can be taken.	16. **Ongoing Monitoring** – Conduct ongoing monitoring and periodic reviews of the internal control systems effectiveness. The monitoring should involve internal and external resources (as appropriate). 17. **Reporting** – Results of the ongoing monitoring and review should be reported to management and the board (and other relevant stakeholders) in a timely manner, in particular if deficiencies have been identified and/or changes to the existing systems are required.

Monitoring and Review of Internal Control Systems

15. The board is responsible for putting in place a proper process and procedures to govern the ongoing monitoring and periodic reviews of the issuer's risk management and internal control systems[79].

[79] MDR paragraph H and Principle D.2.

16. The board may delegate the monitoring and control activities to board committees, management, and internal and external functions. The board should, however, maintain oversight and apply independent and professional judgment on any reports it receives on the effectiveness of the risk management and internal control systems. The board should also consider whether the issuer in its particular circumstances may benefit from the engagement of independent third parties (such as external auditors or consultants) to facilitate the ongoing monitoring or the periodic reviews.

17. The CG Code requires issuers to conduct reviews of the risk management and internal control systems' effectiveness at least annually[80]. The board should assess the frequency and scope (e.g. whole or parts of the systems) of the review, taking into account the particular situation of the issuer. For example, more frequent reviews may be appropriate where significant control failings and weaknesses were identified in prior reviews, and review intervals of one year may be too long for assessing the effectiveness of the adopted remedial measures.

18. The board should plan how the review should be conducted and how relevant work will be distributed among the issuer's management and internal departments and external providers. The board is also responsible for ensuring that the review process is adequately resourced. It is important to document and keep a record of the steps taken, and the outcome of the review of the risk management and internal control systems' effectiveness (including any assurance that the board has received).

Scope for annual reviews

19. The scope for the review of risk management and internal control systems should be broad and cover all material aspects of these systems, including financial, operational and compliance controls[81]. It should also cover the issuer's subsidiaries.

20. The areas of focus below represent matters that may be considered for review. To the extent that any area is not included within any review, a clear record should be kept of the reasons for determining not to do so.

[80] MDR paragraph H and Principle D.2.
[81] CP D.2.1.

Table 7: Scope for annual reviews of risk management and internal control systems[82]

Components	Scope for Annual Review
Component 1 - Corporate culture / control environment	**Assessment of integrity and ethical values across the organization, including:** What are the relevant policies and procedures (including on code of conduct, conflict of interest, whistleblowing, handling of complaints); what is the approach to legal and regulatory compliance (including compliance with the Listing Rules and the CG Code); how is staff / management remuneration assessed. **Assessment of board independence and performance, including:** What is the level of independence, experience and respective roles and responsibilities of board members; is there a process for the declaration of interest; what is the composition of the board committees; whether the terms of reference of the board committees remain appropriate and what is the level of communication between the board and its committees; are directors' interests being declared. **Assessment of management performance and commitment to internal controls, including:** What is the quality of financial reporting (including but not limited to relevance, reliability, comparability and timeliness); what are the operational goals and policies & procedures in pursuit of such goals; is there sufficient attention to and frequency of discussions on governance, risk and internal control related topics. **Assessment of organizational structure, including:** What are the relevant legal entities, business units, etc. and their responsibilities; how do the reporting lines (in particular between management and business units) work. **Assessment of financial reporting competencies, including:** What is the level of staffing and is the experience and qualification of staff members adequate, in particular in relation to governance / financial reporting; what is the level of training. **Assessment of responsibilities and delegation, including:** What are the relevant roles and responsibilities, level of authority, assignment of authority and delegation, relevant policies and procedures (including on override of authority).

[82] Source: The Hong Kong Institute of Certified Public Accountants, Technical Bulletin, Assistance Options to New Applicants and Sponsors in connection with Due Diligence Obligations, including Internal Controls over Financial Reporting.

	Assessment of human resources performance, including: What policies and procedures are in place, what is their practical implementation in relation to recruitment, training, performance evaluation, promotion, compensation, termination. **Assessment of legal / regulatory compliance, including:** What is the level of compliance with (i) (financial) reporting requirements, (ii) laws and regulations (including Listing Rule compliance), and what are the internal control systems in place to procure such compliance, and monitor and report potential deficiencies.
Component 2 - Risk assessment	**Assessment of objectives, including:** Are there clear objectives in terms of the issuer's operations / business, financial reporting and regulatory / legal compliance. **Assessment of risk assessment and management procedures, including:** What are the processes in place for risk assessment and management; regulatory and legal compliance; fraud identification and prevention; is there an ongoing monitoring of the operating environment and potential risks; are there (business) contingency plans; are financial reporting risks assessed.
Component 3 - Internal controls	**Detailed assessment of internal controls in place, including:** Analysis of policies and procedures, relevant roles and responsibilities, segregation of duties, record keeping and an assessment of compliance with laws / regulations across all aspects of the issuer's operation, such as: • Sales, accounts receivable and collection; • Procurement, accounts payable and payment; • Inventory management, including logistics; • Production and costing; • Human resources and payroll; • Fixed assets; • Cash and treasury management; • Insurance; • Financial reporting and disclosure controls; • Taxes; and • IT system (general and application) controls.
Component 4 - Information and communication	**Assessment of use of information and existing level of communication in relation to:** • Corporate planning, budgeting, forecasting; • Reporting from and to management (including without limitation monthly updates to the board as required by the CG Code);

	• Internal communication, including policies / procedures for monitoring and detecting confidential / sensitive information, possible conflicts, notifiable / connected transactions (Chapters 14 and 14A of Listing Rules), other legal or regulatory exposure; • External communication, including policies / procedures on communication with external parties, distribution of annual/ interim reports and publication of results announcements (including pursuant to Listing Rules 13.46, 13.48 and 13.49), handling of inside information and leakage of sensitive information (including pursuant to Listing Rule 13.09 and Part XIVA of the Securities and Futures Ordinance (Cap. 571 of the Laws of Hong Kong)), regulatory enquiries (including pursuant to Listing Rule 13.10); • Level of confidentiality applied to communication and dissemination of (sensitive) information; and • Level of data protection across the organization, including against cyber threats and data theft, and compliance with applicable personal data laws.
Component 5 - Monitoring	**Assessment of monitoring functions, policies and procedures, including:** • Board / management level monitoring; • Internal audit (or other function) monitoring, including: o Role / responsibility of monitoring function; o Interaction with external auditor / providers; o Evaluation and mitigation of deficiencies; o Escalation / reporting to management / board; o Implementation of internal controls / policies. • Channels for reporting / whistleblowing; • Management letter and internal control findings communicated by external auditor and/or service providers; and • Level of monitoring of legal / regulatory compliance.

Practical considerations for disclosure on risk management and internal controls

An issuer needs to make detailed disclosure in the corporate governance report on its risk management and internal control systems and the (at least) annual reviews of these systems (MDR paragraph H). An issuer should consider the following questions when preparing disclosures:

Disclosure on risk management and internal control systems' scope

- Are there sufficient details on how the issuer identifies and manage significant risks (including ESG, fraud and cyber risks)?
- Is there disclosure on whether the issuer has an internal audit function (and if not, how relevant functions have otherwise been delegated)?
- Is there a description on the relevant aspects of its risk management and internal control systems and any significant changes that were made to the systems during the last reporting period? There should be an explanation on what prompted changes made to the systems (e.g. change in risk profile, discovery of potential deficiencies).

Disclosure on reviews of risk management and internal control systems

- Is disclosure sufficiently detailed on the scope (e.g. which group entities are being included), process and frequency of the review(s) of the risk management and internal control systems conducted during the relevant reporting period?
- Is any description on the roles of all stakeholders involved in the reviews provided (including confirmations whether external providers have been involved)?
- Have the findings and results of the review been disclosed in sufficient detail – including information on any significant control failings or weaknesses identified during the reporting period and remedial steps taken?

Board confirmation of risk management and internal control systems' effectiveness

- Has the board obtained sufficient information and assurances to come to a finding that the issuer's risk management and internal control systems remain effective, including from management, internal departments (e.g. internal audit) or any external provider (e.g. the auditor)?
- Has the board confirmed in the corporate governance report that (i) it is responsible for the issuer's risk management and internal control systems; and (ii) based on the board's review and assurances received, these systems continue to be appropriate and effective?

Policies and systems on whistleblowing and anti-corruption

21. A commitment to integrity, including measures to prevent corruption and to raise concerns and complaints in confidence and anonymity, are key aspects of good corporate governance. Issuers are required to maintain a whistleblowing policy and a policy / system that promotes and supports anti-corruption laws and regulations[83].

22. The Hong Kong Independent Commission Against Corruption (**ICAC**) is developing an Integrity Compliance Management System (**ICMS**), with relevant guidance, that it aims to publish in 2026. The ICMS provides a comprehensive framework of integrity policies and measures to help build an issuer's capacity to uphold integrity and detect and prevent corruption. Issuers are encouraged to adopt the ICMS by integrating relevant procedures into their existing framework of risk management and internal controls. The core components of an ICMS are set out below:

Table 8: Overview of an Integrity Compliance Management System

Core Components	Description
Component 1 - Integrity policy and code of conduct	Implement an integrity policy that covers (among other things): • a statement of top-level commitment to adopt ethical and anti-corruption business practices, high standards of integrity and a zero tolerance for corruption; • the issuer's commitment to capacity building and collaboration with government, regulators, anti-corruption agencies, other corporations, etc. in combating corruption; and • details as to the issuer's anti-corruption measures (see Anti-corruption Policy in Table 9 below). Implement a code of conduct (or update existing one) to set out the required conduct of issuer's directors, management and other staff, including: • compliance with applicable laws and regulations in Hong Kong and abroad; • restrictions on solicitation, acceptance and offering of advantages; • declaration and management of conflicts of interest; • confidentiality of information; and • consequences of breaching the code of conduct.
Component 2 - Integrity capacity and culture building	Adopt practices and measures to build the issuer's integrity capacity and culture:

[83] CPs D.2.6 and D.2.7.

	• embed integrity and ethical values into corporate culture by fostering leadership commitment, communication, accountability and transparency; • adopt regular training focused on integrity capacity building for directors, management and staff at different levels of the issuer; • update existing systems, internal controls and incentives to ensure that integrity becomes an integral part of daily business operations; and • engage with external stakeholders (e.g. government, regulators, anti-corruption agencies, industry peers, business counterparts) on capacity building, sharing of best practices and combatting corruption.
Component 3 - Integrity risk management	Adopt (or update existing) risk management and internal controls to cover: • integrity and corruption risks identification, assessment and management across all areas of the issuer's business (e.g. procurement); and • specific controls for mitigating integrity and corruption risks.
Component 4 - Corruption detection and reporting	Adopt procedures in the issuer's daily operations for corruption detection and reporting, including: • controls and measures for detecting irregularities, misconduct and corruption risks; • procedures for reporting corruption in accordance with the issuer's whistleblowing policy (see Whistleblowing Policy in Table 9 below), including requirements for relevant staff to duly assess each report received; and • procedures for referrals of alleged or suspected corrupt practices to anti-corruption agencies (e.g. the ICAC or relevant overseas anti-corruption agencies) as soon as possible.
Component 5 – ICMS audit	Conduct regular monitoring and periodic "audits" of the implementation of the ICMS by the issuer's internal audit function or other responsible internal department to ensure its effectiveness and consider the need for changes / enhancements.

23. Issuers are required to adopt effective whistleblowing and anti-corruption policies and procedures, either as part of the ICMS or as individual policies. The table below provides further details on what such policies are expected to cover.

Table 9: Overview of Whistleblowing and Anti-corruption Policies

	Whistleblowing Policy	Anti-corruption Policy
Purpose	• Allowing employees and third parties (those who deal with the issuer, e.g. customers and suppliers) to voice concerns. • Safeguarding the confidence and anonymity of concerns raised. • Detecting and deterring misconduct or malpractice.	• Establishing a system of comprehensive anti-corruption measures and procedures in support of applicable anti-corruption laws and regulations. • Providing employees and third parties with clear guidance and requirements on the issuer's anti-corruption policy and applicable anti-corruption laws and regulations. • Promoting anti-corruption culture within the issuers to sustain integrity management and enhance corruption prevention.
Culture / pledge	• Referencing corporate culture / regulatory objectives and commitment to integrity. • Encouraging a "speak-up culture", where concerns on actual or suspected misconduct can be reported. • Confirming confidence and anonymity for any reports made under the policy, and protection from retaliation. • Confirming commitment that complaints / reports will be handled in a timely, fair and independent manner.	• Referencing corporate culture / regulatory objectives and confirming board / management commitment to integrity, zero tolerance for corruption and a "speak-up culture". • Linking anti-corruption policy and procedures with other corporate governance policies and whistleblowing policy / relevant reporting channels. • Confirming the issuer's commitment to compliance with applicable anti-corruption laws in Hong Kong and abroad, including the Prevention of Bribery Ordinance (Cap. 201 of the Laws of Hong Kong).
Personnel to which the policy applies	• Defining who can (i) make whistleblowing reports, and (ii) be subject of such reports (i.e. reporting parties and implicated parties). **Note:** The scope has to be wide to cover board, management, employees at all levels including subsidiaries, and external providers (e.g. suppliers, contractors) and customers (as applicable).	• Defining who is covered by policy. **Note:** The scope should cover the board, management and employees at all levels, including for subsidiaries, external parties doing business with the issuer and those acting in an agency or fiduciary capacity on behalf of the issuer (e.g. agents, consultants and contractors).

Conduct / breaches covered	• Defining breaches or (mis)conduct that warrant reporting under policy (supported by practical examples of major and minor misconduct). • Specifying level of substantiation and evidence expected in support of reports made under the policy.	• Defining breaches or (mis)conduct to which the policy applies (supported by practical examples). • Confirming a prohibition of offering advantages to / soliciting or accepting advantages from any person or organisation in relation to the issuer's business. • Defining any exception to the above prohibition (in accordance with applicable laws) and any approval processes required. • Defining guidelines for the avoidance of actual, perceived or potential conflicts of interest and for the declaration and management of conflicts of interest. • Specifying steps and processes to conduct third-party due diligence.
Implementation / enforcement	• Providing convenient and anonymous channel(s) for reporting. **Note:** (i) Consider whether different channels with different mandates should be established (e.g. for different departments / different group companies / different levels of staff). (ii) While reporting channels should provide anonymity, consider including a statement encouraging reporting person to provide name and/or contact details to facilitate subsequent follow-up actions. • Confirming process of handling reports and involved departments, staff (including any external providers that may be involved in certain functions under the policy). **Note:** Reports against senior management and the board may require handling by a designated staff member with sufficient seniority and independence.	• Confirming process for detecting, assessing and inquiring into possible breaches / misconduct. • Defining disciplinary sanctions resulting from breaches. • Identifying responsible departments / employees overseeing the policy (including any external providers may be involved in certain functions under the policy). • Clarifying when and under which circumstances breaches / misconduct should be (i) escalated to relevant law enforcement agencies (e.g. when reporting to the ICAC is required in respect of alleged or suspected corruption) and (ii) brought to the board's attention. • Providing contact points if queries as to scope and application of the policy arise.

	• Clarifying when reports should be escalated to relevant law enforcement agencies (e.g. the ICAC for corruption-related reports). • Setting out how reports and follow-up actions under the policy are recorded and stored (i.e. through classifying such records as "confidential" and storing them securely to avoid unauthorised access). **Note:** The implementation and operation of the whistleblowing policy should be monitored by the audit committee (or another committee comprising a majority of INEDs).	• Referencing whistleblowing channels available to report possible breaches / misconduct. **Note:** Issuers should ensure that their own inquiries into possible misconduct or breaches of applicable policies / law do not hinder or jeopardise investigations by law enforcement agencies. In particular, where reports have already been made to such agencies, issuers should ensure they align their inquiries with the agency or (where necessary) terminate their own inquiry in order not to impede the agency's investigation.
Communication of policies	• Policies on integrity management, business ethics, governance and compliance, including whistleblowing and anti-corruption policy, have to be regularly communicated to staff of internal departments and external providers (as required) and should be disclosed on the issuer's website. • Reporting channels under the whistleblowing policy should be clearly communicated to staff and easy to access with the necessary level of confidentiality / anonymity.	
Training / capacity building	• Issuers should adopt a systematic approach to enhancing their corporate governance and commitment to integrity to ensure that relevant policies and procedures are implemented in the issuer's daily operations. • This should include periodic training on corporate governance (including on the relevant policies and procedures for anti-corruption and relevant channels for whistleblowing reports). • Training and guidance should be tailored to requirements of different levels of staff and departments, and may be extended to third parties (e.g. customers, suppliers, affiliates, or providers). • Directors should be encouraged to attend regular integrity training, including that offered by the ICAC.	
Review and update of policies	• Regular review and update of relevant corporate governance policies, including the whistleblowing and anti-corruption policy to ensure they stay fit for purpose.	

24. Issuers may approach the ICAC (https://cpas.icac.hk/) for a free, tailor-made and confidential corruption prevention advisory service when shaping and formulating their whistleblowing and anti-corruption policies, systems and procedures. The ICAC also offers:

    - helpful guidance and resources (including "Integrity and Corruption Prevention Guide on Managing Relationship with Public Servants"); and
    - a free subscription to its latest updates, alerts, trainings and publications at: https://subscription.icac.org.hk/subscribe/.

25. Issuers may also make reference to:

    - publications and guidance by other regulators, including the SFC (including the "Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations)"); and
    - other applicable international standards, including the ISO 37001 "Anti-bribery Management Systems" and "The FATF Recommendations" for a comprehensive framework of measures in order to combat money laundering and terrorist financing.

26. For more helpful links and guidance, please visit the External Resources page of the Exchange's Corporate Governance Portal.