Introduction

This is the second in a series of Guidance Notes designed to assist members of The Hong Kong Institute of Chartered Secretaries (HKICS) and the wider profession and community in bribery and corruption compliance. The first Guidance Note in the series provided an overview of the regulatory requirements relating to bribery and corruption in Hong Kong, Mainland China and internationally. This second Guidance Note will cover the key elements of effective bribery and corruption compliance.

An effective ethics and compliance programme is essential for managing bribery and corruption risks in an organisation. It helps to prevent and detect unlawful conduct and to promote a culture that encourages ethical conduct and a commitment to compliance with the laws and local regulations. An effective ethics and compliance programme provides management with timely and accurate information about potential legal problems and allows management to promptly address them.

There are a number of key elements which contribute to the effectiveness of an ethics and compliance programme. These elements are largely consistent across companies, regardless of the industries they operate in.

Tone at the top and middle management

A strong foundation based on the commitment and endorsement of company leaders is vital to the success of an ethics and compliance programme. Management should set the right tone and be seen to play an active and visible role in demonstrating ethical behaviour.

The governing body of an organisation, that is the board of directors, is the starting point for setting the right tone. The board is responsible for ensuring that policies, systems and procedures relating to ethics and compliance are in place and in monitoring the implementation and effectiveness of the programme.

It is crucial that members of the board are actively involved, not only in the monitoring of the ethics and compliance programme, but also in understanding the culture in the organisation and encouraging correct behaviour. Some of the ways in which the board can assist in setting the right tone are:

- members should attend board meetings on a regular basis
- an ethics committee should be established to monitor ethics and compliance issues and be responsible for reporting to the full board
- members should review, consider and evaluate the information provided by management to the ethics committee, escalated to it, or directly where there is no ethics committee
- members should inquire further when presented with questionable circumstances or potential issues
- any potential compliance issue must be addressed, and
- members should promote and encourage ethics and compliance training.

In order for an ethics and compliance programme to work effectively, it is important to engage compliance officer with the authority and resources to manage the programme on a day-to-day basis. The compliance officer should also have direct communication with those ultimately responsible for corporate conduct, including the board of directors.
Building an ethical culture based on principles
A rules-based approach to an ethics and compliance programme would set out the minimum standards of behaviour and practice, and may provide clarity about what is expected of each member of the board. However, this approach also tends to encourage individuals to focus on the rules rather than the principles at stake and they may be more at risk of finding ways around the rules.

Although an effective ethics and compliance programme should contain rules prohibiting illegal behaviour, its primary focus should be on proper actions or effects that should be achieved rather than behaviour to be avoided. An ethical culture that is based on principles and values helps to change mindsets and influence a broad set of practices conforming to the level of expectation of the whole organisation. This would mean that any non-compliance will not really be tolerated by other members of the organisation. The principle and value-based approach also encourages the company to align its ethical culture with best practices and work towards continuous improvement over time.

Implementing the ethics and compliance programme
The real challenge of setting up an ethics and compliance programme is not so much in the design of the framework but in working out how to deliver the right message to the users of the programme – that is, the employees who are responsible for day-to-day operations. Ethical values such as fair and honest competition should be incorporated into the guidelines and instructions and needs to be effectively communicated to the employees.

It is also essential to integrate different divisions into the design process. Without their support in implementing a robust and sustainable programme, it may fail. The programme should be flexible and be able to be tailored to different countries and, more importantly, different cultures.

Board oversight of unethical behaviour
In order to maintain the right tone at the top for the ethics and compliance programme, a demonstration of regular and practical oversight is an essential element. Making an ethics performance evaluation part of the organisation’s standard year-end assessment or creating a strategic plan with an ethics checklist are good tools to assist the board in its oversight.

Supporting whistleblowers
Providing support and incentives to whistleblowers has a long history in the US. Whistleblower protections are also backed by statutes in UK, Europe and the People’s Republic of China. Irrespective of the incentives provided, encouraging all employees to be demanding in the ethical domain is important.

Hong Kong’s Corporate Governance Code addresses this issue. Code Provision C.3.7, for example, indicates that the terms of reference of the audit committee should require a review of the arrangements ‘employees of the issuer can use, in confidence, to raise concerns about possible improprieties in financial reporting, internal control or other matters. The audit committee should ensure that proper arrangements are in place for fair and independent investigation of these matters and for appropriate follow-up action.’

In addition, Recommended Best Practice C.3.8 recommends the audit committee to establish ‘a whistleblowing policy and system for employees and those who deal with the issuer (for example customers and suppliers) to raise concerns, in confidence, with the audit committee about possible improprieties in any matter related to the issuer.’

Risk assessment
The implementation of an effective ethics and compliance programme is more than a matter of simply following a set of rules or providing training. Compliance issues can touch many areas of the business and companies need to know, not only what the highest risks are, but where to marshal the efforts and resources in moving forward. A risk assessment is designed to provide a big picture of the overall compliance obligations and then identify areas of high risk to prioritise limited resources to tackle these high-risk areas first.

Whilst the risks can generally be quantified by two parameters:
1. likelihood of occurrence, and
2. the consequences of occurrence;

there are various ways to categorise different types of risk in commercial or business sectors. Certain typical categories are set out below.

Country risk – What is the correlation between growth markets and corruption risk and what is the perceived level of corruption? The Transparency International Corruption Perceptions Index, or similar list, can provide a benchmark.

Sector and industry risk – Has government publicly stated industry is under scrutiny or already conducted investigations in sector? Are there corruption risks particular to the industry?

Business opportunity risk – Is the business opportunity a high value project for the company? Are there multiple contractors or intermediaries involved in the bidding or contract execution phase?

Business partnership risk – Does this business opportunity require a foreign government relationship? Does a foreign government require the company to rely upon any third parties?
**Transaction risk** – Will the company be required to make any ‘compelled giving’ through any requirements for political or charitable contributions?

**Periodic risk assessments**
In addition to an initial risk assessment to inform the ethics and compliance programme and help the company to identify high risks and prioritise their remediation, risk assessments should be a regular, systemic part of compliance efforts rather than an occasional, ad hoc exercise cobbled together when convenient or after a crisis. They should be conducted at the same time every year and performed by a consistent group, such as the internal audit department or enterprise risk management team. Such annual risk assessments act as a strong preventive measure if they are performed before something goes wrong as it avoids a ‘wait and see’ approach.

There is obviously no single procedure or control which could address all risks to the business and/or mitigate/transfer risk to a reasonably low level. Cost effective compliance procedures should be carefully designed and implemented.

**Historical and emerging risks**
In addition to the traditional risk factors such as contract risk and legal risk, several corporates have suffered from emerging risks including cyber attacks and short-seller attacks. There is still a place for traditional risk assessment approaches when creating awareness and obtaining a quick overview of the risk of the company as a whole. However, the traditional risk assessment may be of limited utility as a source of fresh insights over a period of time. The ethics and compliance programme should be able to extend its risk assessment to newly emerging risks, such as using data analytics to identify new risk indicators.

**Policies and internal controls**
Generally, every company has three levels of standards and controls:

1. **Code of conduct** – every company should have a code of conduct which should express its ethical principles.

2. **Standards and policies** – every company should have standards and policies in place that build upon the foundation of the code of conduct and articulate code-based policies, which should cover such issues as bribery, corruption and accounting practices.

3. **Procedures** – every company should then ensure that enabling procedures are implemented to confirm those policies are implemented, followed and enforced.

**Third party/intermediary management**
The best practices of Foreign Corrupt Practice Act compliance now require companies to have additional standards and controls, including, for example, detailed due diligence protocols for screening third-party business partners for criminal backgrounds, financial stability and improper associations with government agencies. Companies should also perform ongoing monitoring of third parties and intermediaries, and terminate contracts with them if necessary.

**Gifts and hospitality, entertainment expenses, facilitation payments and other sensitive payments**
Gifts and hospitality, entertainment expenses and other sensitive payments are always the focus of typical compliance frameworks and programmes. Note that the US Department of Justice and Securities and Exchange Commission recognise that these expenditures are legitimate if made without corrupt intent, and prosecutions of corporates are unlikely to arise solely from a small, one-off payment of this nature, even if it may appear suspicious. Therefore, there is an emphasis on the corrupt intention. Internal controls must be able to assess what are the purposes of the payments and whether these are legitimate and in a reasonable business context. Note that there is no minimum threshold below which an expenditure will never be viewed as corrupt.

**System of internal control to ensure proper books and record-keeping**
The effectiveness of a good ethics and compliance programme is not indicated by its ability to detect fraud or prevent wrongdoing, but also how fast the programme is able to identify problems and stop employees from damaging the company. While management override of internal controls and failure of segregation of duties remains as two common flaws, a strong and effective system of internal controls is a good line of defence to ensure proper books and record-keeping.

**Communications and continuous reviews of compensation policies**
Although providing incentive and compensation may be an effective way to encourage employees to report misconduct, it is important for the audit committee and management to understand the possible unintended consequences of such rewards.

**Training and communication**
Another pillar of a strong ethics and compliance programme is properly training company officers, employees and third parties on relevant laws, regulations, corporate policies and prohibited conduct. Simply conducting training usually is not enough. Enforcement officials want to be certain the messages in the
training actually get through to employees. The expectations of effectiveness are measured by who a company trains, how the training is conducted and how often the training occurs.

Tailored ethical and compliance training – communication and documentation
Training must be delivered to the right people. The training must prioritise which audience to educate by starting the training programme in higher risk markets and focus on directors, officers and sales employees.

It is a good practice to develop a roadmap and training programme to make the ethics and compliance programme transparent to employees. A well-designed training programme gives members of an organisation the opportunity to practice applying the principles and guidelines to specific, real-life situations they may encounter in their work. The training should also be well-documented in order to keep track with updates and new risks.

Articulate the company’s code of ethics in clear terms
The company’s code of conduct will only have an impact if the appropriate standards of behaviour are effectively communicated to all members of the organisation. Accordingly, the code should be clear and understandable to every employee at every level. Use simple and concise language, and avoid unnecessary legal jargon.

In high-risk markets and for high-risk employees or third parties, live and annual training should be conducted. Enforcement officials have made it clear that live, in-person training is the preferred method in high-risk markets and also that it should be regular and frequent. Another benefit of live training is the immediate feedback from employees that would be much less likely to occur during a webinar or other remote training. Lastly, during the live training, employees are more likely to make casual mention of a potentially risky practices, providing the opportunity to address these before they becomes a larger problem.

Guidance, advice and support available to employees/business partners on complying with company’s code of ethics
One of the best ways to test whether the ethics and compliance programme and code of ethics is working is if employees feel comfortable enough to speak up if they have a concern and whether they believe the company will respond and, if need be, take appropriate action. A company should provide clear and easy to access guidance and advice to its employees on complying with company’s code of ethics or report violations.

Monitoring and evaluating
Monitoring and evaluating have become the basic expectations of ethics and compliance management. There should be a question of whether the company’s employees are adhering to the compliance programme. These ongoing efforts demonstrate the company is serious about compliance. Furthermore, the organisation shall take reasonable steps to demonstrate and ensure that the organisation’s compliance and ethics programme is followed, including monitoring and auditing to detect criminal conduct.

Monitoring tools – data analytics
Monitoring is a commitment to reviewing and detecting compliance programmes in real time and then reacting quickly to remediate them. A primary goal of monitoring is to identify and address gaps in the compliance programme on a regular and consistent basis.

Monitoring the programme is the ongoing surveillance, review, and analysis of key business performance and risk indicators that allows the organisation to identify potential compliance violations. While many seek to implement automatic monitoring programmes, monitoring activities can be either automated, manual or a combination of both.

Data analysis allows a company to re-compute or model the financial recording of transactions, as they ought to be recorded and, therefore, have even greater confidence than if they had tested using sampling. By analysing key assets and related transactions, a company is able to test the entire population and be much more confident and efficient in the results.

Data analytics can transit from a review of historical transaction to a review of current transactions simply by asking similar questions of similar data, but with a change in focus. This is particularly useful on the ongoing monitoring of the compliance programme.

Record-keeping obligations
Data analytics can also be used to assess the effectiveness of internal controls applied on books and record-keeping by analysing the data fields such as date of approval, name of preparer and approver, etc. Auditing is a more limited review that targets a specific business component, region or market sector during a particular timeframe in order to uncover and/or or evaluate certain risks, particularly as seen in financial records. However, it cannot be assumed or viewed as effectively monitoring of compliance programme. A robust programme should include separate functions for auditing and monitoring.
Resources management
Forensic data analytics is dependent on the quality and completeness of the source data. Accordingly, companies should focus on identifying the relevant systems and data relating to the compliance programme.

Incident management and reporting
Incident management is a term describing the activities of an organisation to identify, analyse, and correct hazards to prevent future re-occurrence. Incident management is a very broad concept which involves the assessment of the impacts to the business, including financial, environmental, legal, corporate image, workplace injury, damage or security breaches.

Public relations and media management (including the cyber breach response plan)
Social media represents significant global risk for business enterprises. Companies have responded to this risk by establishing social media compliance policies, but establishing policies is only the beginning of an effort to mitigate social media risk. The massive volume of social media data and the rapid proliferation of a wide variety of social media services necessitates the use of advanced technology to identify and aggregate relevant social media content and understand its implications. Data analytics hold great promise in meeting this need. By understanding what data analytics capabilities are available and how they can be used for compliance purposes, companies can better manage the data preservation and information sharing to the public.

Internal investigation response plan and resources
An internal investigation response plan should be able to understand what has taken place and decide upon appropriate courses of action, such as whether to and how to voluntarily disclose criminal conduct to the government; how to conduct interviews of management and employees, as well as whom to interview; how to treat whistleblowers and cooperating witnesses; how to document the investigation; and how to implement measures to prevent future occurrences.

Internal investigations can be as sensitive as external investigations, especially when they are related to a group of employees or senior management. It is important to design who should be responsible for the investigation and the reporting channels. It is also advisable to secure all communication through a central hub in order to have a better oversight of the information obtained and keep it preserved under privilege.

Disciplinary procedures
Appropriate disciplinary actions could range from a reprimand with additional training, to a demotion or termination of contract. Not to mention, disciplinary action up to and including termination will be taken on a fair and equitable basis and should proportionate to the misconduct convicted.

Confidential reporting
Typical internal reporting channels include telephone hotlines, web-based hotlines, personalised channels for employees, but all of these channels should be private and confidential. Hotline operators should be highly trained to properly debrief the callers.

Remediation plan
A company should remediate problems quickly. A key concept behind the oversight element of compliance is that if a company is policing itself on compliance-related issues, the government will not have to do it for them. Remediation, then, is an important component of oversight. It is not enough to just gather information and identify compliance problems through monitoring and auditing. If improper conduct has been detected, it is imperative that an organisation takes reasonable steps to both address it, and to prevent further similar misconduct.

The members of Ethics, Bribery and Corruption Interest Group are Dr Brian Lo FCIS FCS (Chairman), Lily Chung, Miang Lee and Ralph Sellar. Mohan Datwani FCIS FCS(PE) serves as secretary. Please contact Mohan Datwani, Senior Director and Head of Technical and Research, HKICS, if you have any suggestions about topics relevant to this interest group at: mohan.datwani@hkics.org.hk.

Disclaimer and Copyright
Notwithstanding the recommendations herein, this publication is not intended to constitute legal advice or to derogate from the responsibility of HKICS members or any persons to comply with the relevant rules and regulations. Members and readers should be aware that this publication is for reference only and they should form their own opinions on each individual case. In case of doubt, they should consult their own legal or professional advisers, as they deem appropriate. The views expressed herein do not necessarily represent those of HKICS. It is also not intended to be exhaustive in nature, but to provide guidance in understanding the topic involved. HKICS shall not be responsible to any person or organisation by reason of reliance upon any information or viewpoint set forth under this publication, including any losses or adverse consequences consequent therefrom.

The copyright of this publication is owned by HKICS. This publication is intended for public dissemination and any reference thereto, or reproduction in whole or in part thereof, should be suitably acknowledged.

The Hong Kong Institute of Chartered Secretaries (HKICS) 香港特許秘書公會
(Incorporated in Hong Kong with limited liability by guarantee)