New CIMA Rules & Statements of Guidance to Take Effect in October

Regulatory Update – October 2023

[Reading time: seven minutes]

In April, the Cayman Islands Monetary Authority ("CIMA") released a number of updated rules and guidance; two of which come into effect October 14, 2023. The new rule in respect of Corporate Governance, and the rule and statement of guidance Internal Controls for Regulated Entities. These new rules apply to both mutual and private funds.

So what is the difference between the two documents?

Rules create binding obligations on the regulated entity and breaching the rule may lead to regulatory action, including the imposition of fines and other enforcement penalties. Penalties may be applied against the entity and/or against the operator (directors, managing member, or trustee of a fund or general partner of a fund) or the governing body (directors or managing members of an entity registered under other acts) collectively referenced herein as the "Board").

A Statement of Guidance ("SoG") is, as the title suggests, intended to provide material assistance in complying with rules or with acts of law, or with other documents setting out principles or standards of conduct within the regulated space. SoGs provide a road map demonstrating CIMA's views on compliance with acts, rules and other legislation. If a regulated entity determines not to follow information outlined in a SoG, it is highly recommended that the entity document consideration of the guidance and why it does not apply in the circumstance.

Key Takeaways

1. CIMA expects that the Board members have sufficient time, knowledge and expertise to effect the operation and compliance of the fund.

2. The Board members should exhibit diversity of experience, skills, and knowledge.

3. Board members may delegate functions; however, ultimately, he or she retains accountability for the compliance and overall supervision of the fund.

4. Boards need to consider, document, and approve a code of conduct, conflicts of interest (perceived and actual), personal dealing, outsourcing, private transactions, and preferential treatment with respect to the regulated entity.

5. Internal controls are integral to practices and procedures not add-ons.

6. Reliance on Group policies is acceptable, provided a suitable gap analysis exists to ensure they comply with CIMA requirements.

ComplianceAsia Consulting Limited
Suite 1102, ChinaChem Tower, 34-37 Connaught Road, Central
Tel: (852) 2868 9070
www.complianceasia.com

7. The principle of comply or explain applies, i.e. where a Roard is not following a piece of guidance, it is expected to be documented along with the rationale for non-adoption.

The Rule on Corporate Governance

Like many other pieces of CIMA guidance, the corporate government framework should be commensurate with the size, complexity, nature of business, structure, and risk profile of the entity.

The Rule also recognizes that many CIMA-regulated entities are not generally headquartered in the Cayman Islands are parts of larger groups, often with centralized teams for many functions, including corporate governance. Therefore, it is incumbent upon the Board, to compare the group's policies and procedures against the requirements set down by CIMA and identify any gaps. The results of this gap analysis should be used to tailor a policy, or group policy addendum, to meet the requirements not fulfilled at group level.

The Board is responsible for implementing a corporate governance framework that addresses, at a minimum:

a) Objectives and strategies of the regulated entity
b) Structure of the governance of the Governing Body
c) Appropriate allocation of oversight and management responsibilities
d) Independence and objectivity
e) Collective duties of the Governing Body
f) Duties of individual directors of the Governing Body
g) Appointments and delegation of functions and responsibilities
h) Risk management and internal control systems
i) Conflicts of interest and code of conduct
j) Remuneration policy and practices
k) Reliable and transparent financial reporting
l) Transparency and communications
m) Duties of Senior Management
n) Relations with the Authority

Of all the elements listed above, we would draw your attention to the Structure & Governance of the Board, the Independence & Objectivity of the Board, as well as the need for a Code of Conduct and other governance-related policies.

Most licensed or authorised financial institutions around the world will already have Code of Conduct, usually at a group level with either a local addendum or extra paragraphs to fulfil requirements unique to any given jurisdiction. CIMA expects the Code of Conduct to contain the following key principles, so if these are not mentioned in your group policies, a local addendum may be necessary if the adjustments are not deemed necessary for the master policy:

- Selflessness
- Integrity
- Objectivity
- Accountability
- Openness
- Honesty

ComplianceAsia Consulting Limited
Suite 1102, ChinaChem Tower, 34-37 Connaught Road, Central
Tel: (852) 2868 9070
www.complianceasia.com

- Leadership

As outlined in the beginning of the Rule, group documents are acceptable for use for the Cayman Islands entity, provided a suitable gap analysis has been performed and documented. The same applies to the other policies CIMA expects the Board to put in place: personal dealing, conflicts of interest, private transactions, and the preferential treatment of outside parties.

The Statement of Guidance for mutual and private funds explicitly states that all funds are required to have a conflicts of interest policy.

CIMA expects Boards to be diverse in terms of the fields of expertise, knowledge, and skillsets of the directors, and for them to think, decide, and act independently and objectively. CIMA does acknowledge that internal directors may not have independence in the sense of having no special incentives or vested interests in the activity of the entity and acknowledges that the funds industry sees boards of directors with members of parent companies and fund managers. Nonetheless, it expects these candidates to act solely in the best interest of the entity.

The Board must meet at least annually. The number of annual meetings should be sufficient to allow the Board to monitor operational and regulatory compliance of the entity.

There should be a documented process for the selection and removal of directors, along with a succession plan to ensure continuity of governance.

The Board may delegate powers by appointing outside service providers or by creating sub-committees, however, it cannot delegate its overall responsibility, and especially in the fields of risk management, internal control, internal audit, and, in the case of insurance intermediaries, actuarial matters. To re-iterate, internal audit can be delegated to a third party but the accountability for the exercise of internal audit proceedings remains with the Board.

Rule & Statement of Guidance – Internal Controls for Regulated Entities

This combined document outlines the expectations in respect of internal controls, thus extrapolating on one of the key requirements of the Rule on Corporate Governance and highlights five key internal control principles:

- Control Environment
- Risk Identification and Assessment
- Control Activities and Segregation of Duties
- Information and Communication
- Monitoring Activities and Correcting Deficiencies

In general, this document can be seen as an extension of that Rule since it details CIMA expectations on the roles and responsibilities of the Board and Senior Management, risk management, and the control culture of the entity.

Control culture essentially refers to the ethical operation of the entity, integrity of all staff and of their actions, and the accountability of those assigned the key areas requiring oversight. Control culture also encompasses adequate and fair performance reviews and the adoption of policies and practices

ComplianceAsia Consulting Limited
Suite 1102, ChinaChem Tower, 34-37 Connaught Road, Central
Tel: (852) 2868 9070
www.complianceasia.com

promoting ethical behaviour which do not incentivise risky or unethical behaviour. For example, policies based on achieving performance targets are seen as being contrary to a strong control culture.

Internal controls should form part of an entity's risk management framework and be the basis of policies and procedures, not additional elements. The aim is to make control activities an integral part of day-to-day business, not something which is to be addressed ad hoc, or when the regulating authority asks for information. Such controls include but are not limited to:

- Top level reviews
- Activity controls
- Physical controls
- Compliance with exposure limits
- Approvals and authorisations
- Verifications and reconciliations
- Supervisory controls

Segregation of duties is considered critical to good internal controls, i.e. not concentrating integral (and definitely not conflicting) duties within the remit of the same director or senior manager (if applicable).

Ultimately all internal controls should be regularly reviewed and assessed via an internal audit conducted by appropriately trained and sufficiently independent personnel. This can be outsourced, although the same guidelines in respect of assessing the qualities of the outsourced agent apply.

How regularly these checks are conducted are once again commensurate with the size and complexity of the business. We suggest that at a minimum, relevant businesses should have a rolling two- to three-year internal audit cycle, and as they grow seek shorten the interval until it is conducted annually. For any sized business, additional spot-checks and follow-ups should be conducted between larger scale reviews.

Rule on Cybersecurity

At present the rule does not apply to mutual and private funds, however, it does apply to CIMA Registered Persons under the Securities Investment Business Act. Furthermore, the minimum expectations cited in the Rule are less extensive then the accompanying SOG. For instance, where the SOG recommends the appointment of a Chief Information Security Officer at a senior management level, the Rule stops short of this requirement.

Whereas many similar Rules and/or SOGs may carry the acknowledgment from CIMA that the size and complexity of the organization may not allow for a certain appointment, this is not mentioned in the accompanying SOG. However, the Rule does acknowledge that some firms do outsource information technology-related functions and therefore the Board of Directors is still deemed to be ultimately accountable for the selection of and due diligence on such services providers, along with all cybersecurity issues, including data privacy and protection.

Key considerations of the framework are the role of the directors in overseeing it and ensuring one of the directors is responsible for cybersecurity concerns, the usage and vetting of cybersecurity service providers, training for staff, recovery time objectives, and reporting of incidents to CIMA.

Material cybersecurity incidents must be reported to CIMA within 72 hours of discovery of the relevant incident. These include:

ComplianceAsia Consulting Limited
Suite 1102, ChinaChem Tower, 34-37 Connaught Road, Central
Tel: (852) 2868 9070
www.complianceasia.com

o) Events of material impact to the regulated entity's internal operations.
p) The event results in the unauthorised dissemination of any personal data either internally or externally.
q) Significant operational impact to internal users that is material to customers or business operations.
r) Extended disruptions to critical business systems or internal operations
s) Number of external customers impacted is significant or growing.
t) If determined that there is potential reputational impact, either to the regulated entity or the Cayman Islands as a whole, notification to the Authority must occur immediately if there is any risk of premature public disclosure.
u) Any loss of any card payment information, beneficial owner details, or any personally identifiable information.
v) Loss or exposure of any data in violation of any applicable data protection Acts and other regulatory requirements both foreign and domestic.

About ComplianceAsia

ComplianceAsia, now part of IQ-EQ, is the longest established and largest compliance consulting firm in Asia Pacific, renowned for providing independent and unbiased advice on Asian financial industry rules and regulations. Our client base spans asset managers, hedge funds, private equity funds, family offices, broker-dealers, insurers, wealth management, and investment banks.

As we celebrate a significant milestone of 20 years, we embark on an exciting new journey as part of IQ-EQ, a prominent global investor services group. This strategic collaboration opens doors to a broader range of expertise and resources, enabling ComplianceAsia to expand our current offerings and better support our clients on a global scale.

IQ-EQ has an extensive presence across 25 jurisdictions and a workforce of over 5,000 professionals. By combining their resources with our in-depth knowledge and experience in the Asian market, we create a powerful synergy that will redefine the compliance landscape.

ComplianceAsia Consulting Limited
Suite 1102, ChinaChem Tower, 34-37 Connaught Road, Central
Tel: (852) 2868 9070
www.complianceasia.com

Contact Us Today

HONG KONG SAR

ComplianceAsia Consulting Limited
Suite 1102, ChinaChem Tower
34 - 37 Connaught Road Central,
Central,
Hong Kong

T: +852 2868 9070
E: philippa.allen@iqeq.com

SINGAPORE

ComplianceAsia Consulting Pte. Ltd.
1 Raffles Place,
#27-00 Republic Plaza,
048619,
Singapore

T: +65 6533 8834
E: philippa.allen@iqeq.com

MAINLAND CHINA

ComplianceAsia Shanghai Limited
Room 2955, 29/F, Shanghai Tower,
501 YinCheng Middle Road,
Pudong Xinqu,
200120,
China

E: philippa.allen@iqeq.com
E: rachel.wu@iqeq.com

JAPAN

ComplianceAsia Consulting KK
2603 ARK Hills, Sengokuyama Mori Tower,
9-10 Roppongi 1-Chrome,
Minato-ku, Tokyo,
106-0032,
Japan

E: philippa.allen@iqeq.com
E: james.bailey@iqeq.com
E: manabu.nagano@iqeq.com

www.complianceasia.com

ComplianceAsia