APPENDIX 1

RULE AND STATEMENT OF GUIDANCE

Internal Controls for Regulated Entities

Table of Contents

List of Acronyms

Acronym	Definition
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
CIMA	Cayman Islands Monetary Authority
CPF	Countering the Financing of Proliferation of weapons of mass destruction
MAA	Monetary Authority Act

Rule and Statement of Guidance

Internal Controls for Regulated Entities

1. Introduction

1.1. This document establishes the Cayman Islands Monetary Authority's (the "Authority" or "CIMA") Rule and Statement of Guidance on Internal Controls for Regulated Entities. The Rule and Statement of Guidance should be read in conjunction with the following:

a) CIMA-issued measures on: investment activities of insurers; responsibilities of insurance managers; risk management; corporate governance; market conduct; cybersecurity; records management and retention; internal audit; business continuity management; outsourcing; fitness and propriety; AML/CFT/CPF; and

b) any other regulatory instruments issued by the Authority from time to time.

1.2. This document is broadly organised as follows: Part I sets out the general rules and guidelines for all regulated entities covering each of the five components of internal control, namely: Control Environment; Risk Identification and Assessment; Control Activities and Segregation of Duties; Information and Communication; and Monitoring Activities and Correcting Deficiencies. Part II sets out additional sector-specific rules and guidelines.

2. Statement of Objectives

2.1. To set out the Authority's rules and guidance on the requirements for regulated entities with regards to internal controls. In general, internal controls represent the way a regulated entity is structured and operated so that reasonable assurance is provided of:

a) the ability to carry on its business in an orderly and efficient manner;
b) the safeguarding of its and its clients' assets;
c) the maintenance of proper records and the reliability of financial, operational, and regulatory reports; and
d) the compliance with all applicable acts and regulatory requirements.

2.2. The Authority recognises that internal control needs may vary from one regulated entity to another depending on its structure, size, nature, complexity, and risk profile. Hence, this Rule and Statement of Guidance is not intended to be exhaustive; rather, it sets out the Authority's requirements and minimum expectations on internal controls.

3. Statutory Authority

3.1. This Rule and Statement of Guidance is consistent with Section 34 of the Monetary Authority Act (MAA) which provides that:

"34(1) After private sector consultation and consultation with the Minister charged with responsibility for Financial Services, the Authority may–

(a) issue or amend rules or statements of principle or guidance concerning the conduct of licensees and their officers and employees, and any other persons to whom and to the extent that the regulatory acts may apply;

(c) issue or amend rules or statements of principle or guidance to reduce the risk of financial services business being used for money laundering or other criminal purposes."

3.2. To highlight the Authority's internal control rules within this document, a rule is written in light blue and designated with the letter "R" in the right margin.

4. Scope of Application

4.1. The Rule and Statement of Guidance applies to all entities regulated by the Authority under the regulatory acts (as defined and amended under the MAA); subject to proportional application outlined in paragraphs 4.2 to 4.4 below.

4.2. The Authority recognises that regulated entities may outsource some business functions, delegating their duties for day-to-day management to service providers. A regulated entity may rely on the service providers' system of internal control over the outsourced activities provided that the Governing Body is satisfied and can demonstrate to the Authority that such system of internal control meets the requirements of this Rule and Statement of Guidance[1].

4.3. Where a regulated entity is part of a group, it may rely on the group's system of internal control provided that the regulated entity's Governing Body is satisfied and can demonstrate to the Authority that such system of internal control meets the requirements of this Rule and Statement of Guidance.

4.4. In assessing whether the internal control system implemented or relied upon by a regulated entity meets the requirements of this Rule and Statement of Guidance, appropriate consideration should be given to the structure, size, nature, complexity, and risk profile of the regulated entity.

4.5. References to any act or regulation shall be construed as references to those provisions as amended, modified, re-enacted or replaced from time to time.

5. Definitions

5.1. The following definitions are provided for the purpose of this Rule:

5.2. The **"Governing Body"** of a regulated entity is the Board of Directors where the entity is a corporation, the General Partner where the entity is a partnership, the manager where the entity is a Limited Liability Company, the Board of Trustees where the entity is a trust business, or equivalent.

5.3. **"Senior Management"** includes the most senior staff of the regulated entity, including heads of divisions, and any person who fulfils the functions of a senior manager, by whatever name called. Such functions include actively participating in the daily planning, supervision, administration and execution of a regulated entity's objectives and strategy.

[1] Regulated entities utilising outsourcing should also refer to regulatory measures issued by the Authority on outsourcing.

5.4. **"Management"** means collectively, the Senior Management, middle-level management, and lower-level management of the regulated entity.

6. Enforcement

6.1. Whenever there has been a breach of the rules included in this document, the Authority's policies and procedures as contained in its Enforcement Manual will apply in addition to any other powers provided in the regulatory acts and the MAA.

7. Effective date

7.1. This Rule and Statement of Guidance will come into effect within six months of the date that it is published in the Gazette.

PART I

GENERAL RULES AND GUIDELINES FOR ALL REGULATED ENTITIES

8. Control Environment

The control environment refers to the set of standards, processes, and structures that provide a basis for carrying out effective internal control across the organization. An effective control environment creates the discipline that supports the assessment of risks necessary for the achievement of the entity's objectives, performance of control activities, and use of information and communication systems, as well as the conduct of monitoring activities. The control environment, therefore, has an extensive impact on the overall system of internal control. The Governing Body and Senior Management establish the tone at the top regarding the importance of internal controls and expected standards of conduct. Additionally, the Governing Body and Senior Management communicate their expectations concerning integrity and ethical values throughout the organization and, as appropriate, to outsourced service providers and business partners.

The Role of the Governing Body

8.1. The Governing Body of a regulated entity is ultimately responsible for ensuring that an adequate and effective system of internal control is established, documented, and maintained. R

8.2. The Governing Body is responsible for approving and periodically reviewing the overall business strategies and significant policies of the regulated entity. It should also have the responsibility of understanding the material risks faced by the regulated entity, setting acceptable levels for these risks, and ensuring that Senior Management takes the steps necessary to identify, measure, monitor and control these risks. Additionally, the Governing Body is responsible for approving the organizational structure and ensuring that Senior Management is monitoring the effectiveness of the internal control system. R

8.3. The Governing Body of a regulated entity must demonstrate independence from its Management and exercise oversight of the development and performance of internal controls. Where it is not reasonably possible for the Governing Body to achieve independence from its Management, documented policies and procedures must be in place to identify and manage actual or perceived conflicts of interests. R

8.4. The Governing Body provides governance, guidance, and oversight to Senior Management. Members of the Governing Body should be objective, capable, and inquisitive, with knowledge or expertise of the activities of and risks run by the regulated entity. As appropriate, the Governing Body should consist of some members who are independent from the daily management of the regulated entity. A strong, active Governing Body, particularly when coupled with effective upward communication channels and capable financial, legal, and internal audit functions, provides an important mechanism to ensure the correction of problems that may diminish the effectiveness of the internal control system.

8.5. The Governing Body should include in its activities (1) periodic discussions with Management concerning the effectiveness of the internal control system, (2) a timely review of evaluations of internal controls conducted by Management, internal auditors, and/or external auditors, (3) periodic efforts to ensure that Management has promptly followed up on recommendations and concerns expressed by auditors and/or supervisory authorities on internal control weaknesses, and (4) a periodic review of the appropriateness of the regulated entity's strategy.

The Role of Senior Management

8.6. Senior Management should have responsibility for implementing strategies and policies approved by the Governing Body and developing processes that identify, measure, monitor and control risks incurred by the regulated entity. Additionally, Senior Management should have the responsibility of setting appropriate internal control procedures and monitoring the adequacy and effectiveness of the internal control system.

8.7. A regulated entity must establish, document, and communicate its organisational structure including the appropriate functions, lines of reporting, responsibility, and authority. R

8.7.1. Senior Management, with oversight from the Governing Body, should ensure that there are no gaps in reporting lines and that an appropriate and effective level of management control is extended to all levels of the organization and its various activities. The documented organisational structure should be kept current and any changes appropriately communicated.

8.7.2. Internal control responsibilities can generally be viewed as falling within three lines of defence against the failure to achieve the entity's objectives:

a) Management and other personnel on the front line provide the first line of defence in day-to-day activities. They are responsible for maintaining effective internal control day to day;

b) business-enabling functions such as risk, control, legal, and compliance provide the second line of defence as they clarify internal control requirements and evaluate adherence to defined standards; and

c) Internal auditors provide the third line of defence in assessing and reporting on internal control and recommending corrective actions or enhancements for management consideration and implementation.

8.8. Members of Senior Management typically delegate duties for development of more specific internal control policies and procedures to those responsible for a particular business unit. Delegation is an essential part of management; however, it is important for Senior Management to oversee the managers to whom they have delegated these duties to ensure that they develop and enforce appropriate policies and procedures.

8.9. A regulated entity is required to demonstrate a commitment to ensuring that activities are conducted by persons with sufficient knowledge, skills, and experience commensurate with its structure, size, nature, complexity, and risk profile. R

8.9.1. Staff training and skills should be regularly updated with adequate consideration given to training needs to ensure compliance with the regulated entity's operational and internal control policies and procedures; and compliance with all applicable legal and regulatory requirements to which the entity is subject.

Control culture

8.10. Regulated entities are required to demonstrate a commitment to integrity and ethical values. R

8.10.1. An organization's control environment can also be seen as synonymous with its internal control culture. Elements of a strong culture, such as integrity and ethical values, effective oversight, accountability, and performance evaluations, make the control environment strong as well. Culture is part of an organization's control environment, but also encompasses elements of other components of internal control such as establishing effective policies and procedures, ease of security controls or access to information, and the responsiveness to the results of monitoring activities.

8.10.2. The Governing Body and Senior Management are responsible for promoting high ethical and integrity standards, and for establishing a culture for the regulated entity that emphasises and demonstrates the importance of internal controls to all levels of personnel, outsourced service providers, and business partners. This includes the ethical values that Management displays in their business dealings, both inside and outside the organization. The words, attitudes, and actions of the Governing Body and Senior Management affect the integrity, ethics, and other aspects of the regulated entities' control culture.

8.10.3. In reinforcing ethical values, regulated entities should avoid policies and practices that may inadvertently provide incentives or temptations for inappropriate activities. Examples of such policies and practices may include undue emphasis on performance targets or other operational results, particularly short-term ones that ignore longer-term risks; compensation schemes that overly depend on short-term performance; ineffective segregation of duties or other controls that could allow the misuse of resources or concealment of poor performance; and insignificant or overly onerous penalties for improper behaviours.

8.11. A regulated entity is required to hold persons who have been assigned responsibilities for internal controls accountable for performance of such responsibilities. R

8.11.1. In varying degrees, internal control is the responsibility of everyone in the organization. Almost all employees produce information used in the internal control system or take other actions needed to implement internal controls. An essential element of a strong internal control system is the recognition by all employees of the need to carry out their

responsibilities effectively and to communicate to the appropriate level of management any problems in operations, instances of non-compliance with the entity's code of conduct, or other policy violations or illegal actions that are noticed. This can best be achieved when operational procedures are contained in clearly written documentation that is made available to all relevant personnel. It is essential that all personnel of the regulated entity understand the importance of internal control and are actively engaged in the internal control process.

8.11.2. Where outsourced service providers perform activities for or on behalf of the regulated entity, Management must implement a program, to evaluate the effectiveness of the system of internal control over such activities. Such a program should be commensurate to the nature, complexity and risk profile of the outsourced activity. R

9. Risk Identification and Assessment

9.1. Risk assessment involves a dynamic and iterative process for identifying, measuring, and analysing risks to achieving an organization's objectives. It also forms a basis for determining how the risks will be managed. A precondition to risk assessment is the establishment of risk-related objectives, linked at different levels of the organization. Management should consider the suitability of the objectives established. Risk assessment also requires Management to consider the impact of possible changes in the external environment and within its own business model that may render the internal control system ineffective.

9.2. Regulated entities must specify their objectives with sufficient clarity to be able to identify and assess the risks relating to those objectives. R

9.2.1. Objectives form the basis on which risk assessment approaches are implemented and performed and subsequent control activities are established. As part of internal control, Management may consider specifying and grouping objectives at all levels of the entity within broad categories relating to operations, reporting, and compliance. The grouping of objectives within these categories allows for the risks to the achievement of those objectives to be identified and assessed.

9.3. Regulated entities must identify and continually assess all material risks to the achievement of their objectives and analyse the risks as a basis for determining how they should be managed. This assessment must cover all material risks (including the risk of fraud) facing the regulated entity on a consolidated basis. R

9.3.1. Internal controls should be regularly reviewed and revised to appropriately address any new or previously uncontrolled risks. For example, as financial innovation occurs, a regulated entity needs to evaluate new financial instruments and market transactions and consider the risks associated with these activities. Often these risks can be understood when considering how various scenarios (economic and otherwise) affect the cash flows and earnings of financial instruments and transactions. Thoughtful consideration of the full range of possible problems, from customer misunderstanding to operational failure, will point to important control considerations.

9.3.2. Effective risk assessment identifies and considers internal factors (such as the complexity of the organization's structure, the nature of the organization's activities, the quality of personnel, organizational changes and employee turnover) as well as external factors (such as fluctuating economic conditions, changes in the industry and technological advances) that could adversely affect the achievement of its objectives. As applicable, this risk assessment should be conducted at the level of individual businesses, across the wide spectrum of activities and subsidiaries of the consolidated entity. Effective risk assessment addresses both measurable and non-measurable aspects of risks and weighs costs of controls against the benefits they provide.

9.3.3. The risk assessment process also includes evaluating the risks to determine which are controllable by the regulated entity and which are not. For those risks that are controllable, it is important for the regulated to assess whether to accept those risks or the extent to which it wishes to mitigate the risks through control procedures. For those risks that cannot be controlled, the regulated entity should decide whether to accept these risks or to withdraw from or reduce the level of business activity concerned.

10. Control Activities and Segregation of Duties

Control activities

10.1. Regulated entities must select and develop control activities (including general control activities over technology) that contribute to the mitigation of risks to the achievement of their objectives to acceptable levels. The control activities are deployed through policies that establish what is expected; and procedures that put policies into action. R

10.2. An effective internal control system requires that an appropriate control structure is established, with control activities defined at every business level. These should include: top level reviews; appropriate activity controls for different departments or divisions; physical controls; checking for compliance with any established exposure limits and follow-up on non-compliance; a system of approvals and authorisations; a system of verifications and reconciliations and a system of supervisory controls.

10.3. Control activities are designed and implemented to address the risks that the regulated entity identified through the risk assessment process. These control activities may be preventive or detective in nature and may encompass a range of manual and automated activities. Control activities involve two steps: (1) the establishment of control policies and procedures; and (2) verification that the control policies and procedures are being complied with. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. Examples of control activities include, but not limited to:

a) **Top level reviews –** The Governing Body and Senior Management often request presentations and performance reports that enable them to review the entity's progress toward its goals. For example, Senior Management may review reports showing actual financial results to date versus the budget. Questions that Senior Management generates as a

result of this review and the ensuing responses of lower levels of management represent a control activity which may detect problems such as control weaknesses, errors in financial reporting or fraudulent activities.

b) **Activity controls -** Department or division level management receives and reviews standard performance and exception reports on a daily, weekly, or monthly basis. Functional reviews occur more frequently than top-level reviews and usually are more detailed. As with the top-level review, the questions that are generated from reviewing the reports and the responses to those questions represent the control activity.

c) **Physical controls -** Physical controls generally focus on restricting access to tangible assets, including cash and securities. The control activities include physical limitations, dual custody, and periodic reconciliation of inventories with control records.

d) **Compliance with exposure limits** – Where applicable, the establishment of prudent limits on risk exposures is an important aspect of risk management. For example, compliance with limits for borrowers and other counterparties reduces concentration of credit risk and helps to diversify a regulated entity's credit risk profile. Consequently, an important aspect of internal controls is a process for reviewing compliance with such limits and follow-up on instances of non-compliance.

e) **Approvals and authorisations** - Requiring approval and authorisation for transactions over certain limits ensures that an appropriate level of management is aware of the transaction or situation and helps to establish accountability. It also affirms that a transaction is valid (i.e., it represents an actual economic event or is within an entity's policy).

f) **Verifications and reconciliations** - Verifications of transaction details and activities; and the verification of output of any risk management models used by the regulated entity are important control activities. Periodic reconciliations, such as those comparing cash flows to accounting records and statements, may identify activities and records that need correction. Consequently, the results of verifications and reconciliations should be reported to the appropriate levels of management whenever problems or potential problems are detected.

g) **Supervisory Controls** - Supervisory controls assess whether other transaction control activities (i.e., activity controls, exposure limits, verifications, reconciliations, authorizations and approvals, physical control activities etc.) are being performed completely, accurately, and according to policy and procedures.

10.4. Control activities are most effective when they are viewed by Management and all other personnel as an integral part of, rather than an addition to, the daily activities of the regulated entity. When controls are viewed as an addition to the day-to-day activities, they are often seen as less important and may not be performed in situations where persons feel pressured to complete activities in a limited amount of time. In addition, controls that are an integral part of the daily activities enable quick responses to changing conditions and avoid unnecessary costs. As part of fostering the appropriate control culture within

the regulated entity, Senior Management should ensure that adequate control activities are an integral part of the daily functions of all relevant personnel.

10.5. It is not sufficient for the regulated entity to simply establish appropriate policies and procedures for its various activities and divisions. Management, with Governing Body oversight, must regularly ensure that all applicable divisions of the regulated entity follow such policies and procedures and determine that existing policies and procedures remain adequate.

Segregation of duties

10.6. A regulated entity must ensure that there is adequate segregation of duties commensurate to its structure, size, nature, complexity, and risk profile. R

10.7. Where segregation of duties is not reasonably practical, a regulated entity must establish and implement appropriate alternative control activities. R

10.8. Segregation of duties is typically built into the selection and development of control activities. When selecting and developing control activities, Management should consider whether duties are appropriately divided or segregated among different persons to reduce the risk of error or inappropriate or fraudulent actions. Such consideration should include the legal environment, regulatory requirements, and stakeholder expectations. This segregation of duties generally entails dividing the responsibility for approving transactions, recording them, and handling the related asset(s).

10.8.1. In some instances, segregation of duties may be not practical, cost effective, or feasible. For instance, small entities may lack sufficient resources to achieve ideal segregation, and the cost of hiring additional staff may be prohibitive. In these situations, management should institute appropriate alternative control activities including, but not limited to: rotation of duties; increased Management oversight such as additional reviews and reconciliations; and third-party involvement, including outsourcing.

10.9. Assigning conflicting duties to one individual (for example, though not limited to, responsibility for both the front and back offices of a trading function) gives that person access to assets of value and the ability to manipulate financial data for personal gain or to conceal losses. Consequently, certain duties within a regulated entity's organization should be split, to the extent possible, among various persons to reduce the risk of manipulation of financial data or misappropriation of assets. There should also be periodic reviews of the responsibilities and functions of management and staff to identify areas of potential conflict of interest and ensure there are independent checks to minimise the risk of concealment of inappropriate actions.

11. Information and Communication

11.1. Regulated entities must obtain or generate, and then use relevant and quality information from both internal and external sources to support effective functioning of internal controls. R

11.2. Information is necessary for an entity to carry out its internal control responsibilities to support the achievement of its objectives. Communication

refers to the continual, iterative process of providing, sharing, and obtaining necessary information internally and externally. Internal communication is how information is disseminated throughout an entity, flowing up, down, and across the entity. It enables Senior Management to communicate internal control responsibilities across the entity. External communication enables inbound communications of relevant external information and outbound provision of information to external parties in response to requirements and/or expectations.

11.3. From the regulated entity's perspective, for information to be useful, it must be relevant, reliable, timely, accessible, and provided in a consistent format. Information includes internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making and functioning of internal controls. Internal information is part of a record-keeping process that should include established procedures for record retention.

11.4. An effective internal control system requires that there are reliable information systems in place that cover all significant activities of the regulated entity. These systems, including those that hold and use data in an electronic form, must be secure, monitored independently and supported by adequate contingency arrangements.

11.4.1. Regulated entities should be particularly aware of the organizational and internal control requirements related to processing information in an electronic form and the necessity to have an adequate audit trail. Management decision-making and effectiveness of internal control could be adversely affected by unreliable or misleading information provided by systems that are poorly designed and controlled.

11.4.2. Electronic information systems and the use of information technology have risks that must be effectively controlled by regulated entities to avoid disruptions to business and potential losses. Since transaction processing and business applications have expanded beyond the use of mainframe computer environments to distributed systems for mission-critical business functions, the magnitude of risks also has expanded. Controls over information systems and technology should include both general and application controls. General controls are controls over computer systems (for example, mainframe, client/server, and end-user workstations) and ensure their continued, proper operation. General controls include in-house back-up and recovery procedures, software development and acquisition policies, maintenance (change control) procedures, and physical/logical access security controls. Application controls are computerised steps within software applications and other manual procedures that control the processing of transactions and business activities. Application controls include, for example, edit checks and specific logical access controls unique to a business system. Without adequate controls over information systems and technology, including systems that are under development, regulated entities could experience loss of data and programs due to inadequate physical and electronic security arrangements, equipment or systems failures, and inadequate in-house backup and recovery procedures.

11.4.3. In addition to the risks and controls above, inherent risks exist that are associated with the loss or extended disruption of services caused by factors beyond the regulated entity's control. In extreme cases, since the delivery of corporate and customer services represent key transactional, strategic, and reputational issues, such problems could cause serious difficulties for regulated entities and even jeopardise their ability to conduct key business activities. This potentially requires the regulated entity to establish business resumption and contingency plans using an alternate off-site facility, including the recovery of critical systems supported by an external service provider. The potential for loss or extended disruption of critical business operations requires an institution-wide effort on contingency planning, involving business management, and not focused on centralised computer operations. Business resumption plans should be periodically tested to ensure the plan's functionality in the event of an unexpected disaster.

11.5. Regulated entities must have effective internal channels for communicating information on objectives and responsibilities necessary to support the proper functioning of internal control. R

11.5.1. An effective internal control system requires effective channels of communication to ensure that all staff fully understand and adhere to policies and procedures affecting their duties and responsibilities and that other relevant information is reaching the appropriate personnel.

11.5.2. Senior Management of regulated entities should establish effective paths of communication to ensure that the necessary information is reaching the appropriate people. This information relates both to the operational policies and procedures of the regulated entity as well as information regarding its actual operational performance.

11.5.3. The organizational structure of the regulated entity should facilitate an adequate flow of information - upward, downward and across the organization. A structure that facilitates this flow ensures that information flows upward so that the Governing Body and Senior Management are aware of the business risks and the operating performance of the entity. Information flowing down through an organization ensures that the entity's objectives, strategies, and expectations, as well as its established policies and procedures, are communicated to lower-level management and operations personnel. This communication is essential to achieve a unified effort by all employees to meet the regulated entity's objectives. Finally, communication across the entity is necessary to ensure that information that one business line or department knows can be shared with other affected divisions or departments.

12. Monitoring Activities and Correcting Deficiencies

12.1. Regulated entities must establish and implement appropriate processes for monitoring the effectiveness of their internal controls. R

12.2. Monitoring activities assess whether each of the five components of internal control is present and functioning effectively to support the achievement of the organization's objectives. Monitoring is a key input of the organization's

assessment of the effectiveness of internal control. It also provides valuable support for assertions of the effectiveness of the system of internal controls.

12.3. As an entity's operating environment may be dynamic and rapidly evolving, it is important for regulated entities to continually monitor and evaluate their internal control systems in the light of changing internal and external conditions and enhance these systems as necessary to maintain their effectiveness. Senior Management should ensure that the monitoring function is properly defined and appropriate for structure, size, nature, complexity, and risk profile of the regulated entity.

12.4. Monitoring the effectiveness of internal controls can be done by personnel from several different areas, including the business function itself, financial control, and internal audit. For that reason, it is important that Senior Management makes clear which personnel are responsible for which monitoring functions. Monitoring of effectiveness of internal controls should be ongoing, as part of the daily activities of the regulated entity but could also include separate periodic evaluations as appropriate. The frequency of monitoring different activities of a regulated entity should be determined by considering the risks involved and the frequency and nature of changes occurring in the operating environment.

12.4.1. Ongoing monitoring activities can offer the advantage of quickly detecting and correcting deficiencies in the system of internal controls. Such monitoring is most effective when the system of internal controls is integrated into the operating environment and produces regular reports for review. Examples of ongoing monitoring include the review and approval of journal entries, and management review and approval of exception reports.

12.4.2. In contrast, separate evaluations typically detect problems only after the fact; however, separate evaluations allow an entity to take a fresh, comprehensive look at the effectiveness of the internal control system and specifically at the effectiveness of the monitoring activities. These evaluations can be done by personnel from several different areas, including the business function itself, financial control, and internal audit. Separate evaluations of the internal control system often take the form of self-assessments when persons responsible for a particular function determine the effectiveness of controls for their activities. The documentation and the results of the evaluations are then reviewed by Senior Management. All levels of review should be adequately documented and reported on a timely basis to the appropriate level of management.

Internal audit

12.5. As applicable, there should be an effective and comprehensive audit of the internal control system carried out by operationally independent, appropriately trained, and competent staff.

12.6. The internal audit function, as part of the monitoring of the system of internal control, should report directly to the Governing Body or its audit committee, and communicate its findings and recommendations to Senior Management. The internal audit function should have appropriate standing within the regulated entity to ensure senior management acts upon its recommendations.

12.7. The internal audit function is an important part of the ongoing monitoring of the system of internal controls because it provides an independent assessment of the adequacy of, and compliance with, the established policies and procedures. It is critical that the internal audit function is independent from the day-to-day functioning of the regulated entity and that it has access to all activities conducted by the regulated entity including, where applicable, at its branches and subsidiaries.

Internal control deficiencies

12.8. Regulated entities must ensure that internal control deficiencies, whether identified by business line, internal audit, or other control personnel, are reported in a timely manner to the appropriate parties for corrective action. All significant internal control deficiencies must be reported to Senior Management and the Governing Body of the regulated entity. R

12.9. Reporting on internal control deficiencies depends on the criteria established by Governing Body, Management, and other parties such as regulators and standard-setting bodies, as applicable. Results of ongoing and separate evaluations are assessed against those criteria to determine whom to report to and what is reported.

12.10. Once internal control deficiencies and ineffectively controlled risks are reported, it is important that Management corrects the deficiencies on a timely basis. Senior Management should be responsible for establishing an appropriate system to track internal control weaknesses to ensure that actions to rectify the weaknesses are carried out on a timely basis. As applicable, the internal audit function should conduct follow-up reviews or other appropriate forms of monitoring, and immediately inform Senior Management or the Governing Body of any uncorrected deficiencies.

12.11. Regulated entities should have adequate procedures for receiving, recording, investigating, monitoring, and resolving complaints from customers. A high number of complaints may indicate inadequate controls or undue override of existing controls. Therefore, regulated entities should ensure complaints are handled fairly, consistently, and timely and that necessary action is taken to sufficiently remediate the control deficiencies highlighted by the complaints.

12.12. The Governing Body and Senior Management should periodically receive reports summarising key control issues that have been identified and/or complaints received. The reports should include information such as nature of issues, volume, frequency, how the issues were addressed, and disciplinary actions undertaken for non-compliance. Issues that appear to be immaterial when individual control processes are looked at in isolation, may well point to trends that could, when linked, become a significant control deficiency if not addressed in a timely manner.

PART II
SECTOR-SPECIFIC RULES AND GUIDELINES

A. TRUST COMPANIES, COMPANY MANAGERS AND CORPORATE SERVICES PROVIDERS

1. Introduction and Scope of Application

1.1 The purpose of this part of the Internal Controls Rules and Guidelines is to establish the obligations and provide some guidance specifically for the regulated entities in the fiduciary service sector. The regulated entities covered in Section A of Part II are (1) trust companies; (2) company managers; and (3) corporate services providers.

1.2 This sector-specific guidance addresses specialised areas that require more and/or different guidance or explanation than dealt with in Part I of this Rule and Statement of Guidance and should be read in conjunction with Part I.

2. Definitions

2.1 The following definitions are provided for the purpose of this section:

a. **"Client"** refers to a person with whom the regulated entity has entered an agreement to provide services constituting trust business or company management business. Where the regulated entity is a Trust, Restricted Trust or Nominee Trust, "Client" may also refer to a beneficiary of any trust administered by a Trust, Restricted Trust or Nominee Trust.

b. **"Client money"** includes money that a regulated entity holds or receives on behalf of a Client or owes to a Client.

3. Operational Controls

3.1 As applicable, a Client's assets must be segregated from other Clients' assets and from those of the regulated entity. R

3.2 Client money must be held in clearly segregated and distinct accounts from other Clients' accounts and any accounts of the regulated entity. R

3.3 Regulated entities must ensure appropriate written disclosure to Clients on the terms upon which Client money is held. R

3.4 Regulated entities must ensure that Client money accounts are reconciled promptly. R

3.5 Appropriate authorisation and signing powers, at a minimum, dual signatory in the event of Client money pay-outs shall be implemented, subject to Client agreed terms and conditions. R

3.6 Regulated entities shall implement policies and procedures to prevent, subject to Client agreed terms and conditions, inappropriate use of Client money including the use of such Client money for the settlement of the regulated entity's fees and disbursements. R

B. SECURITIES INVESTMENT BUSINESS

1. Introduction and Scope of Application

1.1. The purpose of this part of the Internal Controls Rules and Guidelines is to establish the obligations and provide some guidance specifically for regulated entities in the securities investment business sector. The regulated entities covered in Section B of Part II are securities investment business licensees and registered persons undertaking the regulated activities of market makers, broker-dealers, securities arrangers, securities advisors, and securities managers.

1.2. This sector-specific guidance addresses specialised areas that require more and/or different guidance or explanation than dealt with in Part I of this Rule and Statement of Guidance and should be read in conjunction with Part I.

2. Definitions

2.2 The following definitions are provided for the purpose of this section:

a. **"Client"** refers to a person with or for whom securities investment business is transacted.

3. Operational Controls

3.1. Regulated entities must establish appropriate policies and procedures to minimize the potential for the existence of conflicts of interest between the regulated entity or its personnel and Clients. In circumstances where actual or apparent conflicts of interest cannot reasonably be avoided, Clients must be fully informed of the nature and possible ramifications of such conflicts and in all cases, treated fairly. R

3.2. Where a regulated entity exercises discretionary authority over a Client's account, procedures must be established to ensure that the precise terms and conditions under which such authority may be exercised are effectively communicated to the Client, and that only transactions which are consistent with the investment strategies and objectives of the relevant client, are effected on the Client's behalf. R

3.3. Regulated entities must establish and maintain appropriate and effective procedures in relation to dealing and related review processes to prevent or detect errors, omissions, fraud and other unauthorised or improper activities, and which ensure the fair and timely allocation of trades effected on behalf of Clients. R

3.4. Regulated entities must ensure that Client funds and property are clearly segregated from funds and property of the regulated entity. R

SIX, Cricket Square
PO Box 10052
Grand Cayman KY1 - 1001
CAYMAN ISLANDS

General Office: 345-949-7089

www.cima.ky