|  |  |  |  |
| --- | --- | --- | --- |
| **Procedure:** |  Systems and Controls | **From (date):** |  October 2023 |
| **Replacement?:** |  Y | **Produced by:**  |  Essentials |
| **Signed off by:**  |  (SMF16)  |

Systems and Controls procedure

**Description of the procedure to be carried out**

On an annual basis, the Compliance Manager must carry out an audit of appropriate systems and controls within the firm for the purpose of establishing risk, with and without the firm, and detailing measures to be taken to eliminate/mitigate those risks.

**Individuals who are required to carry out this procedure**

SMF16

**Individuals responsible for ensuring that this procedure is carried out**

SMF16

**Circumstances under which procedure must be carried out**

Annually.

**Arrangements for monitoring**

The form, or assessment sheet, must be retained and completed as any necessary actions are carried out to demonstrate robust governance.

**Standard to be met**

Principle 3 of the FCA Handbook, which requires us to take reasonable care to organise and control our affairs responsibly and effectively.

Senior management arrangements, systems and control

* + 1. Each year the Compliance Officer will complete the appropriate systems and controls self audit form for the purpose of establishing risk with and without the firm.
		2. FCA/PRA requires that we have in place senior management arrangements and systems and controls that are appropriate to manage our business:
			- We encourage directors and/or senior managers to take practical responsibility for matters that are likely to be of interest to FCA/PRA, because they impact on FCA/PRA objectives (see section 2);
			- We adhere to Principle 3, which requires us to take reasonable care to organise and control our affairs responsibly and effectively; and
			- Wherever possible we vest responsibilities in specific named directors and/or senior managers.

Senior management

* + 1. We ensure that at least two members of the company’s senior management (names) must be involved in both the formulation and implementation of the company’s policies. Each individual has sufficient experience and knowledge of the business and the necessary personal qualities and skills to detect and resist any imprudence, dishonesty or other irregularities by the other individual.

**Staff Structure**

* + 1. The headcount of the company is number. We ensure that each role has a clear competency based job description to allow for accountability and responsibility. The structure of the operation is set out elsewhere in the procedures.

**Key personnel and controlled functions**

Governance

* + 1. The following are our governance arrangements: We ensure at all times that we have
	+ A clear organisational structure;
	+ Consistent & transparent lines of responsibility;
	+ Effective processes to manage & monitor risk;
	+ Effective processes to manage & monitor consumer outcomes;
	+ Sound administrative & accounting procedures; and
	+ Effective safeguards for IT processing.
		1. At all times we take reasonable care to maintain a clear and appropriate apportionment of significant responsibilities among our directors and senior managers. We monitor and control business and affairs through these directors, senior management and governing body (in this case our Board).
		2. We have apportioned our responsibilities as follows

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Executive | Compliance | Money Laundering | Advice | Insurance Mediation |
|  |  |  | ? advisers |  |
|  External - TCD |

* + 1. In addition we have delegated certain activities to outsourced enterprises as follows

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Accounts | HR | IT | Compliance support | Compliance Audit |
|  |  |  | TCD |  |

**Governance and oversight**

* + 1. Our governance and oversight structure is provided by the board and Compliance Officer.
		2. There is no external auditing requirement.
		3. We have adopted full Fitness and Propriety policies and procedures for all regulatory staff, and employ personnel with the skills, knowledge and expertise necessary for the discharge of the responsibilities allocated to them (see 1.7 above).
		4. Our systems and controls around recruitment enable us to satisfy the board of the suitability of anyone who acts for the company. This includes assessing an individual's honesty, integrity and competence. This assessment will be made at the point of recruitment and assessed regularly thereafter. Appropriate procedures have been prepared to ensure that staff remain both competent and suitable for the roles allocated to them.
		5. We understand that, where [employees](file:///C%3A%5CFSA%5Cglossary-html%5Chandbook%5CGlossary%5CE%3Fdefinition%3DG365) who are not subject to an examination requirement in the FCA’s rules to pass a relevant examination, we need to demonstrate that the [employee](file:///C%3A%5CFSA%5Cglossary-html%5Chandbook%5CGlossary%5CE%3Fdefinition%3DG365) satisfies the knowledge component of the [competent employees rule](file:///C%3A%5CFSA%5Cglossary-html%5Chandbook%5CGlossary%5CC%3Fdefinition%3DG2498) relating to his / her job. Our procedures mirror the FCA’s own requirements when assessing the fitness and propriety of a [person](file:///C%3A%5CFSA%5Cglossary-html%5Chandbook%5CGlossary%5CP%3Fdefinition%3DG869) to perform a particular job. The most important considerations will be the [person's](file:///C%3A%5CFSA%5Cglossary-html%5Chandbook%5CGlossary%5CP%3Fdefinition%3DG869):

(1) honesty, integrity and reputation;

(2) competence and capability; and

(3) financial soundness.

Systems and Controls

* + 1. We take reasonable care to establish and maintain such systems and controls as are appropriate to our business tempered by the:
			- nature, scale and complexity of our business;
			- volume and size of our transactions;
			- risk of our firm being used to further financial crime; and
			- degree of risk associated with each area of its operation.
		2. These systems and controls are set out in the following sections:
			- Risk assessment
			- Audit
			- Remuneration Policies
			- Record keeping
			- Business Continuity

Risk assessment

* + 1. The Compliance Officer (supported by outsourced compliance) is responsible for the control of the risk of non-compliance with the FCA regulations as well as the proper management of operational risk. The company has highlighted the following key risks to its business:
			- Operational risk (which includes risk arising from failed internal processes, people and systems);
			- Outsourcing, and
			- External events having an impact on the business strategy.

The organisational structure and internal control model for the company is designed to be fully consistent with FCA requirements. The Board has adopted a strategy of a “Three Lines of Defence Approach” to mitigate risks and establish its internal framework. This approach is set out below:

* + 1. The First Line of Defence is the framework of policies and procedures that we have put in place, covering all key operations.

The Second Line of Defence is the Risk Management measures (collection of relevant management information evidencing compliance with procedures) the management team adhere to.

The Third Line of Defence is the review of the company operations and risk management operations by the FCA, through thematic reviews and regulatory reporting.

**Risk**

* + 1. The company’s overall risk management framework is maintained annually by the Compliance Officer and defines risks and risk limits that are either acceptable or unacceptable to the company. Any area that is considered a potential risk is assessed by the management team and, if necessary, action is taken to bring the particular risk within tolerances.

Remuneration policies

* + 1. From time to time the company’s remuneration policies might lead to conflicts between the requirements or standards that the firm is required to meet and the financial advantage of the individual. Any such tensions are appropriately managed through an annual appraisal of the remuneration structure. The company does not pay its its sales staff a fluctuating emolument other than through a share of profits with discretion regarding the individual’s performance and compliance with the firm’s procedures.

**Record Keeping**

* + 1. The company is required to keep adequate records of matters and dealings that are the subject of requirements and standards under the FCA regime. These records are capable of being reproduced on paper in English. We retain records for at least the minimum lengths of time as determined by specific FCA regulation and are be held in a secured location (electronically on a password protected server).
		2. The Compliance Officer is responsible for maintaining a current list of the company’s record keeping arrangements and monitoring adherence to the requirements in the relevant sections of the FCA Handbook.
		3. Details of the records to be kept, and for how long they must be retained, can be found in the [SUP Schedule 1](http://www.fshandbook.info/FS/html/FCA/SUP/Sch/1) and in [COBS Schedule 1](http://www.fshandbook.info/FS/html/FCA/COBS/Sch/1).
		4. The Compliance Officer is responsible for maintaining records of:
			- Financial promotions including advertisements (which are required to be final proof copies) – see separate financial promotions procedure for detail. In relation to advertisements specifically, records must be retained for three years [five years for MiFID business] from the date of last issue (COBS 4.11.1).
			- Updates to the compliance procedures; and
			- Procedures for ensuring that the Compliance Manual is kept up-to-date and available to all members of staff.
			- All measures taken to monitor and record Consumer Duty related procedures, outcomes and rationale behind corrective actions taken.
		5. The Compliance Officer has overall responsibility for all complaints received by the company.
		6. A delegated member of staff (name) maintains a record of where all relevant documentation is held and in what form.
		7. Before destroying any records, or removing them so that they cannot be retrieved within the specified time, the company will refer to the requirements of [SUP Schedule 1](http://www.fshandbook.info/FS/html/FCA/SUP/Sch/1) and [COBS Schedule 1](http://www.fshandbook.info/FS/html/FCA/COBS/Sch/1).
		8. The records may be kept in the form of a hard copy or any other form that is readily accessible and capable of prompt reproduction in hard printed form.
		9. In the case of a subject access request under the Data Protection Act, the company must enable a customer to inspect any and all records relating exclusively to them within 40 days of the request.
		10. If a customer requests records which do not concern only him, the company may refuse to comply but must inform the customer that the FCA/PRA has the right to inspect them.

See further detail under the specific Data Protection procedure.

* + 1. All staff are specifically made aware regularly that, without express written consent, no record or file is to be amended or destroyed if it may be relevant to any matter which is currently the subject of an inspection, investigation etc.
		2. The implication of this is that back ups are required for all information retained on disk or tape, and also that information should be capable of retrieval in its original format.

**Business Continuity**

* + 1. The company has prepared a Business Continuity / Disaster Recovery document. The Compliance Officer is responsible for maintenance of the document. Its purpose is to ensure that, in the case of an interruption to its systems and procedures, any losses are limited, essential data and functions are preserved, and the maintenance of its [regulated activities](file:///C%3A%5CFSA%5Cglossary-html%5Chandbook%5CGlossary%5CR%3Fdefinition%3DG974), or, where that is not possible, the timely recovery of such data and functions and the timely resumption of its [regulated activities](file:///C%3A%5CFSA%5Cglossary-html%5Chandbook%5CGlossary%5CR%3Fdefinition%3DG974), is achieved. In summary, the business continuity policy covers:
* Resource requirements such as people, systems and other assets, and arrangements for obtaining these resources;
* The recovery priorities for the company ’s operations;
* Communication arrangements for internal and external concerned parties (including the FCA, [customers](file:///C%3A%5CFSA%5Cglossary-html%5Chandbook%5CGlossary%5CC%3Fdefinition%3DG156) and the press);
* Recovery in relation to the key outsourced functions (as applicable) of the company;
* Escalation and invocation plans that outline the processes for implementing the business continuity plans, together with relevant contact information;
* Processes to validate the integrity of information affected by the disruption; and
* Regular testing of the business continuity policy in an appropriate and proportionate manner.
	+ 1. The main objective of the plan is to recover all business critical processes and minimise the impact for the company’s employees, customers and reputation. Implementing a plan requires careful preparation and planning. The Compliance Officer role is to ensure all the steps outlined in this procedure are followed and the plan is updated on a regular basis.