Banking Newsletter

Number 5 Year 1997

Financial Services Commission

Guidance Note on Accounting & Other Records and Internal Control Systems

Introduction

1 The maintenance of adequate accounting and other records of its business and adequate systems of control of its business and records is one of the statutory criteria for licensing under the Banking Ordinance 1992[1].

2 In addition, licensed banks must maintain adequate records to :

(a) enable the directors of locally incorporated licensees to fulfil their statutory duties in relation to the preparation of accounts; and

(b) ensure that directors and management have complete, accurate and timely information to enable them to make returns to the Commissioner of Banking or the Banking Supervisor in a proper and prompt fashion; and to enable them to furnish them with any other information which might reasonably be required.

3 It is the responsibility of an institution's directors and management to ensure that adequate records and systems are maintained and the responsibility of the Commissioner of Banking to judge whether the criterion for licensing relating to those records and systems is satisfied.

4 The Commissioner of Banking will rarely find it appropriate to prescribe the manner in which a particular institution should maintain its accounting and other records and internal control systems. Rather, this newsletter emphasises the scope and nature of the financial information which the accounting and other records must be designed to capture, contain and provide for management and emphasises the scope and nature of the internal control systems and the purposes for which they are established by management.

Part 1 : Accounting And Other Records

5 The scope and nature of the accounting and other records which are required for the business to be conducted in a prudent manner should be commensurate with an institution's needs and particular circumstances and should have regard to the manner in which the business is structured, organised and managed, to its size and the nature, volume and complexity of its transactions and commitments. The accounting and other records should be located where they will best assist management to conduct the business of the institution in a prudent manner on a day-to-day basis. If the accounting and other records of a Gibraltar branch of an overseas-incorporated institution are kept outside Gibraltar there should be arrangements which allow local management to have immediate access to them.

[1] Section 23(3)(h).

General Requirements

6 It is not appropriate to prepare a comprehensive list of the accounting and other records which an institution should maintain. However, the accounting and other records should meet the following general requirements:-

(a) capture and record on a timely basis and in an orderly fashion every transaction and commitment which the institution enters into with sufficient information to explain:-

(i) its nature and purpose;

(ii) any asset and/or liability, actual and contingent, which respectively arises or may arise from it; and

(iii) any income and/or expenditure, current and/or deferred, which arises from it;

(b) provide details, as appropriate. for each transaction and commitment, showing:-

(i) the parties including, in the case of a loan, advance or other credit exposure, whether and if so to whom it is sub-participated;

(ii) the amount and currency;

(iii) the contract, rollover, value and settlement or repayment dates;

(iv) the contracted interest rates of an interest rate transaction or commitment;

(v) the contracted exchange rate of a foreign exchange transaction or commitment;

(vi) the contracted commission or fee payable or receivable together with any other related payment or receipt;

(vii) the nature and current estimated value of any security for a loan or other exposure; the physical location and documentary evidence of such security; and

(viii) in the case of any borrowing, whether it is subordinated and, if secured, the nature and book value of any asset upon which it is secured;

(c) be maintained in such a manner that financial and business information can be extracted promptly to enable management to:-

(i) monitor the quality of and safeguard the institution's assets, including those held as custodian;

(ii) identify, quantify, control and manage its exposures by related counterparties across all products;

(iii) identify, quantify, control and manage its exposures to liquidity risk and foreign exchange and other market risks across all products;

(iv) monitor the performance of all aspects of its business on an up-to-date basis; and

(v) make timely and informed decisions;

(d) contain details of exposure limits authorised by management which are appropriate to the type, nature and volume of business undertaken. These limits should, where relevant, include counterparty, industry sector, country, settlement, liquidity, interest rate mismatch and securities position limits as well as limits on the level of intra-day and overnight trading positions in foreign exchange, futures, options, future (or forward) rate agreements (FRAs) and swaps; provide information which can be summarised in such a way as to enable actual exposures to be readily, accurately and regularly measured against these limits;

(e) contain details of the factors considered, the analysis undertaken and the authorisation or rejection by management of a loan, advance or other credit exposure; and

(f) provide on a memorandum basis details of every transaction entered into in the name of or on behalf of another party on an agency or fiduciary (trustee) basis where it is agreed that the institution itself is not legally or contractually bound by the transaction.

Information For Management

7 Every institution should prepare information for directors and management so that they can monitor, assess and control the performance of its business, the state of its affairs and the risk to which it is exposed. This information should be prepared on an individual company and, where appropriate, on a consolidated basis. The frequency with which information is prepared, its level of detail and the amount of narrative analysis and explanation will depend upon the level of management to which it is addressed. Some types of information will be needed on a more frequent basis than others and it may be appropriate for some to be presented on a basis of breaches from agreed limits by way of exception reports.

8 It is the responsibility of directors and management to decide what information is required and to decide who should receive it. Appropriate management information should be provided to:-

(a) persons responsible for exercising managerial functions or for maintaining accounting and other records;

(b) executives who, either alone or jointly, are responsible under the immediate authority of the directors for the conduct of the business of the institution; and

(c) the directors of the institution.

9 This information should be prepared:-

(a) to show the state of affairs of the institution;

(b) to show the operational results of the business both on a cumulative basis and by discrete period and to give a comparison with budgets and previous periods;

(c) to provide an analysis of assets and liabilities showing how they have been valued;

(d) to provide an analysis of its off-balance sheet positions showing how they have been valued;

(e) to provide an analysis of income and expenditure showing how it relates to different categories of asset and liability and off-balance sheet positions; and

(f) to show the institution's exposure to each type of risk, compared to the relevant limits set by management.

Part 2: Internal Control Systems

Introduction

10 The scope and nature of effective control systems should take account of the size of the business, the diversity of operations, the volume and size of transactions, the degree of risk associated with each area of operation, the amount of control by senior management over day-to-day operations, the degree of centralisation and the extent of reliance on information technology. A system of internal control must be designed to provide reasonable assurance that all the institution's revenues accrue to its benefit, all expenditure is properly authorised and disbursed, all assets are adequately safeguarded, all liabilities are recorded, all statutory requirements relating to the provision of accounts are complied with and all prudential reporting conditions are adhered to.

General Requirements

11 It is not appropriate to prepare a comprehensive list of internal control procedures which would then be applicable to any institution nor is it possible to prepare a detailed list of particular procedures which should be undertaken, where appropriate, by all institutions. Nonetheless, internal control systems should provide reasonable assurance that:-

(a) the business is planned and conducted in an orderly and prudent manner in adherence to established policies;

(b) transactions and commitments are entered into in accordance with management's general or specific authority;

(c) management is able to safeguard the assets and control the liabilities of the business; there are measures to minimise the risk of loss from irregularities, fraud and error, and promptly and readily to identify them when they occur;

(d) the accounting and other records of the business provide complete, accurate and timely information;

(e) management is able to monitor on a regular and timely basis, inter alia, the adequacy of the institution's capital, liquidity, profitability and the quality of its assets;

(f) management is able to identify, regularly assess and, where appropriate, quantify the risk of loss in the conduct of the business so that:-

(i) the risks can be monitored and controlled on a regular and timely basis; and

(ii) appropriate provisions can be made for bad and doubtful debts, and for any other exposures both on and off-balance sheet; and

(g) management is able to prepare returns made to the Banking Supervisor completely and accurately and in accordance with the

Banking Supervisor's reporting instructions and to submit them on a timely basis.

12 In seeking to secure reasonable assurance that their internal control objectives are achieved, management must exercise judgement in determining the scope and nature of the control procedures to be adopted. They should also have regard to the cost of establishing and maintaining a control procedure in relation to the benefits, financial or otherwise, that it is expected to provide.

13 It is a responsibility of directors and management to review, monitor and test its systems of internal control on a regular basis in order to assure their effectiveness on a day-to-day basis and their continuing relevance to the business. In many institutions an internal audit function will assist management by providing an independent review of such systems. Such a review should be designed to monitor the effectiveness and operation of the systems and to test compliance with daily procedures and controls (see paragraphs 26-30 below).

Detailed Control Objectives

14 The scope and nature of the specific control objectives which are required for the business to be conducted in a prudent manner should be commensurate with an institution's needs and particular circumstances and should have regard to the manner in which the business is structured, organised and managed, to its size and the nature, volume and complexity of its transactions and commitments.

15 It is not appropriate for the Commissioner of Banking to provide an exhaustive and prescriptive list of detailed control requirements which should apply to all institutions. However, the Commissioner of Banking considers that each institution should address the following control objectives:-

(a) organisational structure;

(b) monitoring procedures;

(c) segregation of duties;

(d) authorisation and approval;

(e) completeness and accuracy;

(f) safeguarding assets; and

(g) personnel.

Organisational Structure

16 Institutions should have documented the high level controls in their organisation, defining and allocating responsibilities, identifying lines of reporting for all aspects of the enterprise's operations, including the key controls and giving outline job descriptions for key personnel. The delegation of authority and responsibility should be clearly specified.

Monitoring Procedures

17 An institution should have procedures in place to ensure that relevant and accurate management information covering the financial state and performance of the institution and the exposures which the institution has entered into are provided to appropriate levels of management on a regular and timely basis. Procedures should also be in place to ensure compliance with the institution's policies and practices including any limits on delegated

authority referred to in paragraph 16, statutory, supervisory and regulatory requirements.

Segregation Of Duties

18 A prime means of control is the separation of those responsibilities or duties which would, if combined, enable one individual to record and process a complete transaction. Segregation of duties reduces the risk of intentional manipulation or error and increases the element of checking. Functions which should be separated include those of authorisation, execution, valuation, reconciliation, custody and recording. In the case of a computer-based accounting system, systems development and daily operations should be separated.

Authorisation And Approval

19 All transactions should require authorisation or approval by an appropriate person and the levels of responsibility should be recorded as prescribed by paragraph 16.

Completeness And Accuracy

20 Institutions should have controls to ensure that all transactions to be recorded and processed have been authorised, are correctly recorded and are accurately processed. Such controls include checking the arithmetical accuracy of the records, checking valuations, the maintenance and checking of totals, reconciliation's, control accounts and trial balances, and accounting for documents.

Safeguarding Assets

21 An institution should have controls designed to ensure that access to assets or information is limited to authorised personnel. This includes both direct access and indirect access via documentation to the underlying assets. These controls are of particular importance in the case of valuable, portable or exchangeable assets and assets held as custodian.

Personnel

22 There should be procedures to ensure that personnel have capabilities commensurate with their responsibilities. The proper functioning of any system depends on the competence and integrity of those operating it. The qualifications, recruitment and training as well as the innate personal characteristics of the personnel involved are important features to be considered in setting up any control system.

Controls In An Information Technology Environment

23 The information held in electronic form within an institution's information systems is a valuable asset that needs to be protected against unauthorised access and disclosure. The control objectives described above apply equally to operations undertaken in both manual and electronic environments although there are additional risks associated with electronic environments. It is the responsibility of management to understand the extent to which an institution relies upon electronic information to assess the value of that information and to establish an appropriate system of controls. The Commissioner of Banking recognises that this will usually be achieved by a combination of manual and automated controls, the balance of which will vary between institutions, reflecting the need for each to address its particular risks cost effectively.

24 The types of risk most often associated with the use of information technology in financial systems may be classified as follows:

(a) **Fraud and Theft**:- Access to information and systems can create opportunities for the manipulation of data in order to create or conceal significant financial loss. Additionally, information can be stolen, even without its physical removal or awareness of the fact, which may lead to loss of competitive advantage. Such unauthorised activity can be committed by persons with or without legitimate access rights.

(b) **Errors**:- Although they most frequently occur during the manual inputting of data and the development or amendment of software, errors can be introduced at every stage in the life cycle of an information system.

(c) **Interruption**:- The components of electronic systems are vulnerable to interruption and failure; without adequate contingency arrangements this can lead to serious operational difficulty and/or financial loss.

(d) **Misinformation**:- Problems may emerge in systems that have been poorly specified or inaccurately developed. These might become immediately evident, but can also pass undetected for a period during which they could undermine the veracity of supposedly sound information. This is a particular risk in systems where audit trails are poor and the processing of individual transactions difficult to follow.

25 Management should be aware of its responsibility to promote and maintain a climate of security awareness and vigilance throughout the organisation. In particular, it should give consideration to:

(a) IT security education and training, designed to make all relevant staff aware of the need for, and their role in supporting, good IT security practice and the importance of protecting company assets;

(b) IT security policy, standards, procedures and responsibilities, designed to ensure that arrangements are adequate and appropriate.

Internal Audit

26 Internal audit is an integral part of the systems of internal control established and maintained by management and may provide independent assurance over the integrity and effectiveness of these systems.

27 The existence, scope and objectives of internal audit are dependent upon the judgement of management as to its own needs and duties, the size and structure of the institution and the risks inherent in its business. Important considerations in assessing the effectiveness of internal audit include the scope of its terms of reference, its independence from operational management, its reporting regime and the quality of its staff (see paragraphs 29 and 30 below).

28 While the Commissioner of Banking does not consider it appropriate at the present time to prescribe that all licensed institutions have an internal audit function, it nevertheless encourages institutions to establish such a function, to facilitate an independent assessment and monitoring of the effectiveness of internal controls. The following control functions could be undertaken by internal audit:-

(a) review of accounting and other records and the internal control environment;

(b) review of the appropriateness, scope, efficiency and effectiveness of internal control systems;

(c) detailed testing of transactions and balances and the operation of individual internal controls to ensure that specific control objectives have been met;

(d) review of the implementation of management policies; and

(e) special investigations for management.

29 It is important to ensure that the internal audit function is appropriately structured and resourced to enable it to provide the independent appraisal of internal controls. There should be clearly defined terms of reference and its independence should be assured by an obligation to report regularly to the audit committee, or in its absence an executive specified by the Board, with the right of access to the audit committee, where one is established. Normally internal audit should not have authority or responsibility for the activities it audits.

30 Internal audit should have unrestricted access to all of an institution's activities, records, property and personnel to the extent necessary for the effective completion of its work. The internal audit function should be staffed with individuals who are appropriately qualified for the function either by holding professional qualifications or by having the requisite experience. Internal auditors should have regard to the Auditing Guideline: Guidance for Internal Auditors issued in June 1990 by the Auditing Practices Committee.

Anti-Money Laundering Systems And Controls

31 Institutions are required by the Criminal Justice Ordinance to establish and maintain specific policies and procedures and training programmes to prevent their businesses and the financial system being used for the purposes of money laundering. In essence, these procedures are designed to achieve two purposes: first; to enable suspicious transactions to be recognised as such and reported to the authorities; and secondly, to ensure that a business can provide its part of the audit trail. The requirements and:

(a) internal controls and communication of policies;

(b) identification procedures;

(c) record keeping;

(d) recognition of suspicious transactions and reporting procedures; and

(e) education and training.

32 The specific requirements that institutions are expected to meet are set out in detail in the Money Laundering Guidance Notes issued by the Financial Services Commission. Copies of these, priced at £5.00 each, can be obtained from the Commission’s offices.

Published by :

Financial Services Commission,
Suite 943, Europort,
PO Box 940,
Gibraltar.

Email : info@fsc.gi
http://www.fsc.gi

Tel (+350) 40283
Fax (+350) 40282

November 1997