MFSA

MALTA FINANCIAL SERVICES AUTHORITY

BANKING UNIT

BANKING NOTICES

NOTICE ON INTERNAL CONTROL SYSTEMS IN CREDIT INSTITUTIONS AUTHORISED UNDER THE BANKING ACT 1994

Ref: BN/03/2002

NOTICE ON INTERNAL CONTROL SYSTEMS IN CREDIT INSTITUTIONS AUTHORISED UNDER THE BANKING ACT 1994

INTRODUCTION

1. The Malta Financial Services Authority as the competent authority ('the authority') appointed under Section 3 (1) of the Banking Act 1994 ('the Act') considers that a system of effective internal controls must be a critical component of the credit institution's management and a basis for sound operations. This will assist a credit institution to meet its objectives and goals, and in the process achieve long-term profitability targets and maintain reliable financial and managerial reporting.

2. It is not the purpose of this Banking Notice ('the Notice') to set specific rules on internal control systems for credit institutions. The authority aims to forward its views on the essential features of an effective internal control system. The Notice is meant to serve as a best practice guideline on how to maintain effective internal control systems. A system of effective internal controls enhances a credit institution's ability to comply with legislation and regulations, and internal policies, rules and procedures, thus decreasing the risk of unexpected losses or impairment to its reputation.

3. The Notice is modelled on the main requisites of a policy paper dated September 1998 and entitled *'The Framework for Internal Control Systems'* issued by the Basle Committee on Banking Supervision.

DEFICIENCIES IN INTERNAL CONTROL SYSTEMS

4. The major sources of internal control deficiencies that may lead to significant losses to credit institutions are briefly described in paragraphs 5 to 9 below.

5. The main deficiencies in internal control experienced by credit institutions can be generally attributed to insufficient commitment by management towards effective internal control systems which is often the result of oversight or accountability through the assignment of roles and responsibilities, and the failure to foster a strong internal control culture within the institution

6. There could be instances in which credit institutions neglect to detect and evaluate the risks of new products and activities or fail to review their risk assessments when there are significant changes in the environment or business conditions. In this regard it must be stressed that control systems that function well for simple financial products may be inadequate for more complex products.

7. A credit institution may fail to install important control structures and activities, such as segregation of duties, authorisations, verifications, reconciliations and reviews of operating performance.

8. Although, at times, internal control structures are in place, lack of knowledge of these policies and procedures by employees and inadequate communication of information between different levels of management, especially the upward communication of problems, leads to such deficiencies.

9. Problems could also arise in instances where internal audit and controls are not sufficient to identify and report weaknesses in the procedures, or, if identified, there is no adequate mechanism to ensure that management rectifies these weaknesses.

THE OBJECTIVES OF INTERNAL CONTROL STRUCTURES

10. Although the responsibility to establish an effective internal control culture lies with the Board of Directors and Senior Management, internal control must be a continuous process within credit institutions. The main objectives of the internal control process, are briefly described below:

Performance Objectives

Internal controls must be geared towards the efficient and effective use of the credit institution's assets and resources and also as a safeguard against losses. The internal control process is to ensure that all employees are working to achieve goals efficiently and with integrity and that their or other interests do not rank prior to those of the institution.

Information Objectives

This objective relates to the preparation of timely, accurate and relevant reports required for the effective decision-making within the credit institution. The information received may be in the form of annual reports, financial statements or related disclosures, and must be reliable, so that it will assist the Board of Directors and Senior Management in the decision making process.

Compliance Objectives

A credit institution must comply with legislation and regulations, supervisory requirements and internal policies in order to safeguard its reputation.

REQUISITES OF AN INTERNAL CONTROL PROCESS

11. The authority recognises that a sound internal control process is critical for a credit institution to meet with established goals and maintain financial viability. The effective functioning of the following key elements of internal control process are therefore imperative to achieve performance, information and compliance objectives.

MANAGEMENT OVERSIGHT

12. The Board of Directors is ultimately responsible to approve and review the overall business strategies and important policies of the credit institution. The Board has also to maintain an effective internal control process, be aware of the major risks facing the institution and to provide guidance and oversight to Senior Management. The Board members must be objective, capable and inquisitive with a good knowledge of the institution's activities and related risks. As stated in Article 40 of the Banking Directive (BD/01) it is recommended that some Board Directors are independent from the daily management of the credit institution.

13. In this regard the activities of the Board of Directors should include:

- ✍ periodic discussions with management regarding the effectiveness of the internal control system;
- ✍ timely review of evaluations of internal controls made by management, internal and external auditors;
- ✍ assurance that the concerns raised by external auditors and supervisory authorities on internal control weaknesses are followed up by management; and
- ✍ periodic reviews to test the adequacy of the institution's strategy and risk limits.

14. Senior Management should be responsible to:

- ✍ implement the strategies and policies approved by the Board to ensure the existence of an effective internal control system. This responsibility is normally delegated, by establishing more specific internal control policies, to particular business units. Notwithstanding such delegation, Senior Management remain responsible to oversee that the managers with the delegated responsibility also develop and enforce appropriate policies and procedures;
- ✍ ensure compliance with the established internal control system. This depends on a well defined organisational structure, which clearly shows the lines of reporting responsibility and authority and provides for effective communication throughout the institution; and
- ✍ ascertain that qualified and competent staff carry out the institution's activities, and that staff training and skills are regularly updated. Effective policies in identifying and recognising employees with the appropriate attitude towards efficient controls may enhance the internal control function. Such policies may also deter those employees who ignore or override existing internal controls.

CONTROL CULTURE

15. The existence of written internal control procedures is not a guarantee that a credit institution will achieve its goals. A strong internal control culture throughout the whole organisation should be ensured by the continuous practical support provided by the Board of Directors and Senior Management and through the consequent effective implementation of such procedures at every level of the institution. The authority is of the opinion that the absence of such a culture may increase the incidence of undetected errors and improprieties.

16. An internal control culture is normally considered effective if:

- ✍ the Board of Directors and Senior Management are exemplary and ethical in their business dealings within and outside the credit institution;

- ✍ employees clearly understand their level of responsibilities in the internal control process. An optimum structure may be possible through the availability of clear written operational procedures to all relevant employees;

- ✍ ethical standards are reinforced if credit institutions avoid introducing policies and practices that unintentionally lead to inappropriate activities. Such policies may include emphasis on performance targets or other operational results, which ignore long-term risks or lead to concealment of poor performance.

RISK RECOGNITION AND ASSESSMENT

17. Credit institutions are in the business of risk taking, and it is therefore imperative that their internal control systems are able to identify and continually assess these risks. The risk assessment process should identify and evaluate internal and external factors that may adversely affect performance, information and compliance objectives. Internal risk factors might include the complexity of internal structure, nature of activities, quality of personnel and turnover and changes within organisation itself, while external risk factors include fluctuation of economic conditions, changes in the industry and technological innovation.

18. Risk assessment is to be conducted in individual business units, and the whole spectrum of activities and subsidiaries of the consolidated credit institution. An effective risk assessment should address both measurable and non-measurable aspects of risk.

19. The risk assessment process should aim to evaluate risks and determine which risks are controllable and those that are not. The credit institution should decide on the acceptable level of controllable risk and the necessary control requirements. This entails the setting up of limits to clearly indicate the *"risk appetite"* in any particular business activity. On the other hand the credit

institution should also decide whether to accept, reduce or withdraw from non-controllable risks inherent to the business activity concerned.

20. Senior Management need to continually evaluate the risks affecting the achievement of the credit institution's objectives and should react to the changing circumstances and conditions. Therefore, when there is financial innovation, management is to evaluate the new financial instruments and transactions for associated risks. The importance of a risk management function within the organisation cannot but be overstressed. The authority is of the opinion that the establishment of independent risk monitoring functions or units will lead to effective risk assessment and continuous monitoring.

CONTROL ACTIVITIES

21. Designed and implemented to address the identified risks through assessment, control activities must form an integral part of the daily activities of a credit institution. The control activities involve the establishment of control policies and procedures and the verification that these policies and procedures are being complied with. The different types of control activities are briefly described below:

Top Level Reviews

The Board of Directors and Senior Management should frequently request and review presentations and performance reports to ensure that the institution is achieving its objectives such as the comparison of budget estimates to the actual financial results. Such reviews should generate queries to lower management. The responses are to be representative of the control activity and therefore may detect control weaknesses, erroneous financial reporting or fraudulent activities.

Activity Controls

Functional reviews at departmental or division level of standard performance and detailed exception reports are to be carried out on a daily, weekly or monthly basis. A practical example is when a commercial lending manager reviews reports on delinquencies, payments received, and interest income earned on a weekly basis. Conversely, a senior credit officer may review such reports on a monthly basis, in a summarised form. Again these reviews should generate questions and answers to assess control weaknesses.

Physical Controls

Such controls are to focus on restrictions to tangible assets, such as cash and securities, through dual custody and periodic inventories.

Compliance with Exposure Limits

Credit institutions are expected to establish prudent limits on risk exposures since this is an important element of risk management. The compliance with

limits for borrowers and other counterparties will reduce the concentration of credit risk and assists to diversify the risk profile. In this respect credit institutions are expected to adopt the criteria established by the Banking Directives and Notices issued by the authority as the minimum required and to strive to implement more stringent limits as deemed necessary within the profile of the institution itself.

Approvals and Authorisations

Transactions over certain limits are to be authorised by the appropriate level of management. This will keep higher management informed of transactions, and moreover establish accountability.

Verifications and Reconciliations

Verification of transaction details and activities and the output of risk management models are important control activities in a credit institution. A relevant example is the periodic reconciliation of cash flows to account records and statements, which may identify activities and records which need correction.

22. Optimum effectiveness from control activities may be obtained if employees view them as an integral part of, rather than an addition to, their daily activities. This procedure may lead the credit institution to a quicker response to changes in conditions and possibly avoid unnecessary costs.

23. Senior Management must be satisfied that all areas of the institution are compliant with established policies and procedures, and that existing policies and procedures remain adequate. This major role is normally carried out by the internal audit function (refer to paragraphs 41-47 of this Notice).

SEGREGATION OF DUTIES

24. Inadequate segregation of duties weakens internal controls and may cause credit institutions to suffer losses. Therefore institutions are expected to ensure that certain duties are segregated, in order to reduce the risk of manipulation of financial data or misappropriation of assets.

25. Possible areas of conflict of interest may exist when an employee performs simultaneously any combination of the following duties:

- ✍ approval of funds and actual disbursement;
- ✍ front, middle and back office duties in a trading function;
- ✍ customer and proprietary accounts;
- ✍ transactions in both the *banking* and *trading books*;

- ✍ informally providing information to customers about their positions while marketing to the same customers;

- ✍ assessing the adequacy of loan documentation and monitoring the borrower after loan origination; and

- ✍ undertaking concurrently a monitoring and executive function.

26. The above list is not exhaustive and credit institution may identify other areas of conflict of interest which have no mitigating factors. All areas of potential conflict therefore need to be identified, minimised and subjected to monitoring by an independent third party.

INFORMATION AND COMMUNICATION

27. The performance of a credit institution's internal control system may be optimised if there is sufficient and effective internal systems for the gathering of information and the dissemination of this information through adequate communication channels. The information should be relevant, timely, accessible and standardised. It may be in the form of financial, operational or compliance including external market information. All information gathered should be relevant and lead to an efficient decision making process.

28. The authority is of the opinion that it is critical for credit institutions to have developed management information systems. These should cover the full range of the institution's activities, and may be in electronic or non-electronic format. Where the information is in an electronic format, the institution should ensure that an adequate audit trail is maintained.

29. Credit Institutions must have effective paths of communication to ascertain that the relevant information is reaching the appropriate employees. The organisational structure of credit institutions has to facilitate the flow of information upward, downward and across the institution. Effective communication ensures the unified effort of all employees to meet the institution's objectives.

MONITORING ACTIVITIES AND CORRECTING DEFICIENCIES

30. As a result of the gathering and dissemination of information, credit institutions should continually monitor and evaluate their internal control systems in order to keep up with the challenges of the dynamic and rapidly evolving industry. Employees from different areas, including the business function, financial control and internal audit have to monitor the system, as part of their daily activities.

31. However additional periodic evaluations of the overall internal control process must be carried out. Ongoing monitoring will assist the quick detection and rectification of deficiencies within the internal control system. Such monitoring is enhanced when integrated into the operating environment and regular reports are issued for review.

32. Credit institutions should have in place procedures for the accurate and timely reporting of identified internal control procedures to the appropriate level of management. Such procedures should cover the reporting of material internal control deficiencies to the Board of Directors.

33. In contrast, separate evaluations normally detect weaknesses in the system after the occurrence. However this allows the Senior Management of credit institutions to have a fresh and comprehensive look at the effectiveness of the internal control systems and specifically at the effectiveness of the monitoring activities. Again employees from different areas, including the business function, financial control and internal audit can carry out these evaluations.

BUSINESS RESUMPTION AND CONTINGENCY PLANNING

34. The objective of a contingency plan is to ensure that a minimum acceptable level of service can be maintained in the event of having to relocate premises due to some unforeseen circumstances. Such a plan would normally consider minor or temporary disruptions as well as major disasters or long term loss of key installations or existing facilities. It is important that contingency plans are tested, tests documented and reinforcements made as necessary. This would minimise the operational risk involved.

35. Credit institutions must retain effective control on their electronic information systems, in order to avoid business disruptions and losses. Since transactions processing and business applications have expanded beyond the use of mainframe computer environments to distributed systems for mission-critical business functions, the magnitude of the risks has also expanded. Information systems and technology controls must cover both general and application controls.

36. General controls are controls over computer systems (e.g. mainframe, client/server, and end-user workstations) to ensure continuous and proper operation. Such controls must include in-house back-up and recovery procedures, software development and acquisition policies, maintenance procedures and physical/logical access security controls.

37. Application controls on the other hand, 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 the business system.

38. Without adequate controls over the information systems and technology, including systems that are under development, credit institutions may 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.

39. Credit institutions must tackle the inherent risk arising from the loss or extended disruption of services caused by factors that are beyond their control. In extreme cases, since the delivery of corporate and customer services represent transactional, strategic and reputational issues, such problems may cause serious difficulties to credit institutions and even endanger their ability to carry out key business activities.

40. Such risks, may in the opinion of the authority, be minimised, if credit institutions 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 are to be periodically tested to ensure functionality in the event of an unexpected disaster.

THE INTERNAL AUDIT FUNCTION

41. The authority requires credit institutions to establish and maintain strong independent internal audit functions, which are properly structured and adequately resourced, in order to facilitate the independent assessment and monitoring of the effectiveness of systems and controls.

42. The Board of Directors and Senior Management are to periodically receive reports, including all the control issues identified. This summarised information may detect significant control deficiencies within the credit institution as opposed to looking at individual control deficiencies which in isolation may look unsubstantial.

43. The Internal Audit function is an important aspect of the ongoing monitoring process of the internal systems of control within the credit institution. This provides an independent assessment of the sufficiency and compliance with current policies and procedures. The authority considers the independence of the audit function from the credit institution's daily activities as critical.

44. The post of Head of Internal Audit is considered as having a key role within the credit institution. Accordingly a suitably qualified and experienced individual is expected to occupy such post.

45. In order to ensure that unbiased information about line activities can be communicated, the Head of Internal Audit should have direct reporting facilities to the Board of Directors, Audit Committee and Senior Management. Internal Audit personnel should be competent, well trained and should clearly understand their duties and responsibilities.

46. The frequency of internal audit reviews is normally consistent with the nature, complexity, and risk of the institution's activities. The independence of the internal auditors may be further enhanced if their resources are allocated by

the Board or top management rather than by managers who are affected by the work of the Internal Audit.

47. All internal control deficiencies or weaknesses in the system are to be immediately reported upon identification. Material matters should be reported to Senior Management and the Board of Directors. It is important that once these reported, credit institutions ensure that deficiencies are corrected on a timely basis. The Internal Audit is to conduct follow-up reviews and appropriate forms of monitoring and immediately inform management, if deficiencies have not been rectified.

AUDIT COMMITTEE

48. The authority favours the establishment of an independent *Audit Committee* to assist the Board of Directors in carrying out its internal control responsibilities. The authority's opinion on the benefits of an effective Audit Committee are given in paragraphs 49 to 55 below.

49. The potential main benefits of an effective Audit Committee are:

- ✍ the improvement in the quality of financial reporting, by reviewing the financial statements on behalf of the Board;
- ✍ the creation of a climate of discipline and control which will reduce the opportunity of fraud;
- ✍ to enable non-executive directors to contribute an independent judgement and play a positive role;
- ✍ to provide a channel for the financial controller and the external auditor to raise issues of concern;
- ✍ to provide a framework within which the external auditor can assert his independence in the event of a dispute with management;
- ✍ the enhancement of the internal audit function, through increased degree of independence from management;
- ✍ to increase public confidence in the credibility and objectivity of financial statements.

50. An Audit Committee is normally constituted as a sub-committee of the Board of Directors, to whom it must be answerable and report regularly. A credit institution is expected to have clear written terms of reference specifying membership, authority and duties of the Audit Committee.

51. The Audit Committee is normally made up of a minimum of three members. Ideally the membership should be mainly confined to non-executive directors

of the credit institution. A majority of the non-executives serving on the Audit Committee should be *independent*[1] of the credit institution.

52. Audit Committee meetings are normally to be attended by the External Auditors, Head of Internal Audit and Financial Director as well as other members of the Board. As a minimum, an Audit Committee must convene twice a year. One meeting should at least be held with the External Auditors and without the presence of any executive Board Members.

53. The credit institution usually grants the Audit Committee explicit authority and the necessary resources and full access to information to enable it to investigate any matters within its terms of reference. The Audit Committee must also be able to obtain non-bank professional advice, and be able to invite to meetings experienced non-bank members.

54. It is advisable that the Audit Committee membership be disclosed in the credit institution's annual report and the Chairman of the Committee would be available to answer questions about its tasks at the Annual General Meeting.

55. The authority recognises the difficulty that small institutions might have in meeting in full the above requirements. In such instances it would be acceptable for the Audit Committee to be structured in a way that would be commensurate with the size of the institution, the volume and the complexity of the institution's transactions and its commitments.

THE ROLE AND RESPONSIBILITIES OF THE EXTERNAL AUDITORS

56. The authority draws attention to the provisions of Section 31 of the Act in relation to communication by External Auditors with the authority itself and to the statutory aspects that are relevant to the external audit function in **respect** of credit institutions. Although the External Auditors do not form part of the credit institution and its internal control systems, they have an important impact on the quality of internal controls through their audit activities. For this reason, the External Auditors may provide important feedback to management on the effectiveness of the credit institution's internal control system, through discussions and recommendations for improvements of current systems.

57. The External Auditors must have a clear view and understanding of the credit institution's internal control systems in order to determine the nature, timing and scope of their audit procedures. The authority believes that this would constitute a solid basis for the external auditors to form their opinion on the annual financial statements of the credit institution.

---

1 As defined in the Licensing Banking Directive (BD/01) the majority of non-executive directors in a credit institution should be independent of management and free from any business or other relationship, which could materially interfere with the exercise of their independent judgement.

58. The authority expects that external auditors adopt professional auditing standards in their audits. Such standards require that audits are planned and performed with the aim of obtaining reasonable assurances that financial statements are free of any material misstatement.

59. The scope, adequacy and effectiveness of a credit institution's internal control systems, including its internal audit function, should be assessed by external auditors and identified weaknesses reported to management accordingly.

60. It is important that all material weaknesses identified by the external auditors are reported to management through confidential management letters.

61. Submissions to the authority of copies of such management letters and other similar in function and replies thereto are a statutory requisite in terms of Section 19(1)(c) of the Act.

62. In view of the role of the authority, the external auditors and the internal auditors within the overall regulatory and supervisory function, the authority considers bilateral and trilateral meetings, as provided for under Section 25 of the Act, as essential for effective liaison between all parties concerned. Such liaison would ensure compliance on a continuous basis with all statutory and regulatory provisions emanating from the Act. Furthermore such meetings would assist the authority in establishing the level of reliance it places on the function of the **internal** and external auditors. Such meetings would also enable the latter to be fully aware of the level of reliance placed upon them by the authority.