

**THE BERMUDA MONETARY AUTHORITY**

**BANKS AND DEPOSIT COMPANIES  
ACT 1999:**

**The Bermuda Monetary Authority's  
Relationship with Auditors and Reporting  
Accountants of Banks and Deposit  
Companies**

## **Introduction**

- 1 This paper sets out the framework and arrangements agreed between the Bermuda Monetary Authority ('the Authority'), the institutions licensed under the Banks & Deposit Companies Act 1999 ('the Act') and the Institute of Chartered Accountants in Bermuda ('ICAB') for the conduct of the relationship between the Authority and the auditors of banks and deposit companies and other accountants who may be commissioned from time to time to report on specific matters under section 39 (1)(b) of the Act. The paper reflects extensive discussion with licensed institutions and with ICAB. It builds on the earlier arrangements, in particular on the code of conduct agreed in 1992 with financial institutions and their auditors, as well as on earlier drafts of this paper dating from 1999, with the most recent being the consultation paper published in December 2006.

## **Legal Background: Auditors**

- 2 The Act requires every licensed institution to appoint annually an approved auditor to audit its financial statements. It also requires licensed institutions to prepare annual financial statements which are to be laid before the members in a general meeting; and it requires the auditor to make a report to members on all annual financial statements which are to be laid in general meetings. It provides that the auditor is to conduct his audit and prepare his report pursuant to the provisions of the Companies Act 1981.
- 3 The Act also sets out particular circumstances in which an approved auditor (and in some cases a licensed institution also) must give written notice to the Authority – in particular, where an approved auditor resigns or does not seek re-election, where the auditor intends to modify his report or qualify his audit opinion in some way, or where he becomes aware that any facts and matters of material significance of the kinds specified in Regulations made under section 60 of the Act may arise.
- 4 Section 39 of the Act provides powers for the Authority to require by notice in writing a licensed institution to provide the Authority with reports on particular matters by its approved auditor or by an accountant or other person with relevant professional skill. Persons appointed by a licensed institution to make such a report are also required, pursuant to this section, to give written notice to the Authority if they become aware that any facts or matters of material significance of the kinds specified in Regulations under section 60 of the Act may arise.
- 5 The specific circumstances triggering the duty by an auditor or accountant to make a report to the Authority are set out in Annex A to this paper. The duty owed under sections 46 (4) and 39 (2) is owed purely to the Authority and not to any other person. At the same time, it is the case that there is no requirement under the Act for an auditor or reporting accountant actively to seek out any possible grounds on which he might be required to make a report under these provisions. Auditors and reporting accountants cannot be expected, in the course of their activities as such, to identify every fact or matter which, had it been known,

would have triggered the reporting obligation to the Authority. Auditors are not expected to change in any way the scope of their audit work, or the frequency or timing of audit visits; nor are reporting accountants expected to vary the scope or depth of their examinations to this end. It is only when they, in the course of their ordinary work, become aware of potentially reportable matters that they need to consider whether they should make further enquiries with a view to determining whether or not they should report a fact or matter to the Authority.

### **Duty of Confidentiality**

- 6 Section 49 of the Act provides a “safe harbour” in respect of matters or concerns disclosed to the Authority by an approved auditor or by a reporting accountant or other expert appointed pursuant to section 39 (1)(b) of the Act. The effect is to ensure that, provided such disclosures are made in good faith, no duty of confidentiality to which the person may be subject shall be contravened by such communication.

### **Relationship Between Supervisors and Auditors and Reporting Accountants**

- 7 The above legal provisions, together with the framework for communication set out in this paper, reflect the importance of ensuring proper dialogue between supervisors and auditors and accountants, in order to reinforce the effectiveness of prudential supervision. It is inherent in the nature of the auditing task that the auditors must assess and make judgments about the quality of the internal control environment within licensed institutions, including in most cases conducting detailed testing of systems and controls. The results of such work can also be highly relevant to the judgments which must be reached by the prudential supervisor: contact between supervisors and auditors therefore strengthens the supervisory system. At the same time, it can help to avoid undue duplication of effort (and hence to minimize unnecessary cost).
- 8 The formal duty placed by the Act on auditors and accountants to report matters to the Authority forms only part of the framework for regular contact and communication between supervisors, auditors and accountants. Equally significant is the commitment of all parties to a frank and constructive dialogue. In particular, the Authority has agreed with licensed institutions that auditors and reporting accountants should have an opportunity to communicate with the Authority routinely within the supervisory process, in relation to the work they have conducted in their capacity as auditors or reporting accountants, including in relation to relevant views and judgments they may have reached in that work. These discussions will occur in regular trilateral meetings involving a licensed institution, its auditor or reporting accountant and the Authority.
- 9 The Authority arranges such trilateral meetings at least once a year, normally shortly after completion of the annual audit process or of any specific work commissioned under section 39 of the Act. Auditors and reporting accountants are expected by their banking clients and

by the Authority to participate fully in such meetings, and to communicate openly with the Authority.

- 10 Trilateral meetings will, as a matter of routine, include discussion of:
  - i. the audit process and any material issues raised by the auditors with the institution arising out of the audit;
  - ii. other relevant issues affecting the preparation or presentation of the financial statements, including material changes in accounting treatment or practice;
  - iii. the operation and effectiveness of internal controls within the institution generally or within a significant group entity or business line;
  - iv. the operation and effectiveness of the internal audit and compliance functions within the institution, including the role and work of the Audit Committee; and
  - v. the operation and effectiveness of the institution's arrangements for the monitoring, management and control of all material risks in its business.

Prior to each meeting, the Authority will prepare and circulate an agenda. Following the meeting, the Authority will also circulate minutes in draft form to the institution and the auditors/accountants for comment, prior to finalizing them.

### **Use of Reporting Accountants and Other Experts**

- 11 The Authority uses its own staff to conduct the greater part of the on-site supervisory work within deposit-taking institutions which is necessary. In particular, the Authority carries out regular compliance visits to licensed firms which provide it with direct insight into a range of aspects of the systems and controls environment. However, the Authority may, in certain circumstances, also require systems and controls reports to be commissioned from reporting accountants. It is not intended that this power be used as a substitute for the routine, on-site inspection reviews carried out by the Authority's own staff. Rather, use of reporting accountants or other skilled persons will be used only where specific concerns arise (for example because of past evidence of serious control lapses), where there may be a need for a more specialised or technical examination (e.g. of an institution's computer systems) or where a serious matter (e.g. a major fraud) needs to be investigated with a degree of urgency that would be possible only by using external, skilled resources. In addition to the licensed institution itself, these reports may also cover systems and controls issues within the wider consolidated Group.
- 12 Reports from reporting accountants are also used as a routine tool to provide a level of assurance as to the completeness and accuracy of the prudential returns which institutions provide to the Authority. This is important in order to offer comfort to the Authority that the information on which it is basing its prudential judgments is accurate. Periodically, therefore, the Authority requires institutions to commission a reporting accountant's report regarding a particular prudential return (or parts of such a return) previously submitted to the Authority, either on a solo or consolidated basis. Material concerns about the accuracy or timeliness of an institution's prudential reporting may, in turn, lead to the

commissioning of further reporting accountant work – for example, assessing the quality of its management information systems.

- 13 As far as possible, the Authority has regard to the views of a licensed institution in determining the choice of reporting accountant who is to carry out a specific commission. Most frequently, the reporting accountant will be an institution's statutory auditor, although another suitable firm may be chosen in certain cases. Examples would include cases in which there may have been concerns about the quality of previous work commissioned from the statutory auditor or where a report calling for particular highly specialized skills may be required.
- 14 Annex B to this paper sets out the agreed arrangements governing the format, content and timing of reporting accountants' reports. Annex C provides an explanation of the Authority's requirements in respect of the accounting, records and internal control systems to be maintained by banks and deposit companies. Annex D sets out the agreed arrangements for reporting accountants' reports regarding prudential returns.

#### **Auditors' Review of Interim Profits**

- 15 Normally, only audited profits are regarded as eligible to be included in the calculation of a licensed institution's capital base for capital adequacy and large exposures' calculation purposes. However, as noted in the Authority's paper The Assessment and Measurement of Capital Adequacy, current year's profits are also eligible for inclusion in tier 1 capital where they have been reviewed by an institution's external auditors. The format that the necessary review and report by the auditors is to take is set out at Annex E.

## ANNEX A

### STATUTORY DUTY TO REPORT TO THE AUTHORITY

Pursuant to sections 46(4) and 39(2) of the Act, together with the relevant Regulations under the Act, the circumstances in which the duty of an auditor or reporting accountant to give written notice to the Authority are as follows:

- i. where an auditor resigns before the expiration of his term of office;
- ii. where an auditor does not seek to be reelected;
- iii. where an auditor decides to include a modification of his report on the institution's financial statements and, in particular, a qualification or denial of his opinion, or the statement of an adverse opinion;
- iv. where an auditor or a reporting accountant becomes aware of any fact or matter which is likely to be of material significance for the discharge, in relation to the institution, of the Authority's functions under the Act.

### Regulations

The relevant Regulations provide a duty to report to the Authority when the auditor or reporting accountant, in the course of carrying out his functions in that capacity:

- i. identifies a material misstatement in the financial statements resulting from fraud, error or illegal acts or the consequences of them;
- ii. concludes that there is substantial doubt as to the ability of the institution to continue as a going concern for a period of one year from the balance sheet date;
- iii. identifies adjustments to the financial statements which individually or in aggregate indicate to him that the previous year's audited annual financial statements or the current year's unaudited interim financial statements, prepared according to generally accepted accounting principles issued to the shareholders were materially misstated, or that the capital adequacy ratio previously calculated for the previous financial year or the current or prior interim period would fall below that set as a minimum by the Authority;
- iv. identifies a material weakness in internal control. A material weakness in internal control is defined as a deficiency in which the design or operation of one or more of the internal control components of the institution does not reduce to a relatively low level the risk that misstatements caused by error or fraud in amounts that would be material in relation to the financial statements being audited may occur and fail to be detected within a timely period by employees in the normal course of performing their assigned functions;
- v. has unresolved disagreements with management pertaining to the application of generally accepted accounting principles that could reasonably be expected to lead in the future to material misstatements of the annual or interim financial

- statements, prepared according to generally accepted accounting principles to be issued to the shareholders in the ensuing financial year;
- vi. identifies any evidence of deliberate attempts by a chief executive or other senior executive to mislead the Authority through the provision of materially false or misleading information; or
  - vii. identifies evidence of fraud or attempted fraud by a chief executive or other senior executive, or has concerns of such a serious nature as to damage materially his confidence in the integrity of the senior management of the institution.

## **ANNEX B**

### **AGREED ARRANGEMENTS FOR THE COMMISSIONING OF REPORTING ACCOUNTANTS' REPORTS UNDER SECTION 39 OF THE BANKS AND DEPOSIT COMPANIES ACT**

- 1 When the Authority decides to require an institution to commission a report under section 39 of the Act, it first draws up an instruction letter which sets out the areas to be reviewed and the timetable which is envisaged for the work. This is discussed with the institution before being circulated to the institution and the reporting accountants as a draft for comment. Ultimately, however, the decision on scope rests with the Authority. When finalised, the Authority writes formally to the institution requiring the work to be commissioned and stipulating the deadlines to be met. The institution must proceed forthwith to commission the report, and write to the Authority confirming that this has been done.
- 2 A section 39 controls report may cover all areas of an institution's business – a so-called “full scope review”. Generally, however, it targets particular areas or aspects, reflecting the risk profile of the institution in question or specific issues or concerns which have arisen. Normally, the reporting accountants are asked to report on aspects of an institution's systems and controls during a specified period. A report providing assurance on prudential returns specifies the particular return or returns which are to be reviewed.
- 3 Unless otherwise agreed in an individual case, reports are to be provided by the reporting accountants to the Board of the commissioning institution within 3 months of the end of the period examined or, if later, within three months of the date of the commissioning letter. The institution then has one month (or such longer period as may have been agreed) to submit the report to the Authority, together with such comments as management may wish to make. Reports are then discussed with institutions and their auditors in trilateral meetings.
- 4 The report should include an outline by the reporting accountants of the steps which they undertook in fulfilling the requirements of the scope of the work set out in the instruction letter. This should include a brief statement as to their procedure, an outline of key tests conducted and of the extent of testing. The report should detail any exceptions found during the review and set out the risks run by the institution in not correcting the particular weakness identified.

## ANNEX C

### **THE AUTHORITY'S REQUIREMENTS FOR ADEQUATE ACCOUNTING, RECORDS AND INTERNAL CONTROL SYSTEMS**

- 1 The Authority's requirements with respect to maintenance of adequate records and systems apply to all aspects of an institution's business. This includes off-balance sheet business, and situations where the institution acts as agent or arranger.
- 2 An institution's Board and senior management need to ensure that the financial record-keeping systems that are in place are capable of providing them and other stakeholders with reliable and timely information. Systems must also be suitable for the preparation and production of audited annual financial statements based on generally accepted accounting principles, together with such interim statements as may be appropriate. Institutions must use valuation rules that are consistent, realistic and prudent, taking account of current values, where relevant.
- 3 The Authority seeks to satisfy itself that institutions' Boards and senior management understand the nature and scale of risk being taken, and make determinations of capital adequacy levels that are consistent with the risk profile. Risk management policies and processes must be appropriate, having regard to the risk appetite and profile, and to the business plan; and they must also be implemented effectively. Effectiveness must be monitored regularly by senior management and the Board, including through review of appropriate risk management information.

#### **Accounting and Other Records**

- 4 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.
- 5 The accounting and other records should be located where they will best assist management to conduct the business of the institution.

Where any such records are kept by another entity (for example, where processing is outsourced) or where records are kept overseas, there should be arrangements ensuring that management have immediate and unrestricted access to them. In addition, there must be no impediment to access by auditors and reporting accountants.

- 6 The Authority sees it as inappropriate to prepare a single comprehensive list of the accounting and other records which an institution should maintain. However, they 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 or liability, actual or contingent, which arises or may arise from it; and
  - (iii) any income or expenditure, current 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) identify, measure, monitor and control the quality of the institution's assets and safeguard them, including those held as custodian;
  - (ii) identify, measure, monitor and control its exposures by related counterparties across all products;
  - (iii) identify, measure, monitor and control 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 should, as appropriate, include counterparty, industry sector, country, settlement, liquidity, interest rate, interest rate mismatch and securities position limits as well as limits on the level of intra-day, overnight trading and open, spot and forward

positions in foreign exchange, futures, options, future (or forward) rate agreements (FRAs) and swaps.

- (e) 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;
  - (f) 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
  - (g) 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.
- 7 Individual companies within the consolidated group should also maintain accounting and other records of a comparable standard.

### **Management Information**

- 8 Every institution should prepare information for the Board and senior management so that they can monitor, assess and control the performance of its business, the state of its affairs and the risks 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 on the level of management to which it is addressed. The Authority maintains under review the adequacy of the institution's systems for measuring, assessing and reporting information on the size, composition and quality of risk exposures.
- 9 It is the responsibility of the Board and senior management to decide what information is required and 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.
- 10 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.

### **Internal Control Systems**

- 11 Institutions must have in place a comprehensive risk management process for identifying, evaluating, monitoring and controlling or mitigating all material risks in their business and enabling them properly to assess the quantum of capital that is appropriate to their risk profile. This process also needs to take into account possible events or changes in market conditions that may adversely affect the institution, including through the use of forward-looking stress-testing techniques. The scope and nature of adequate control systems should take account of:
- (a) the size of the business;
  - (b) the diversity of operations;
  - (c) the volume and size of transactions;
  - (d) the degree of risk associated with each area of operation;
  - (e) the amount of control by senior management over day-to-day operations;
  - (f) the degree of centralisation and the extent of reliance on information technology.
- 12 A system of internal control should be designed and operated to provide reasonable assurance that:
- (a) all the institution's revenues accrue to its benefit;
  - (b) all expenditure is properly authorised and disbursed;
  - (c) all assets are adequately safeguarded;

- (d) all liabilities are recorded;
  - (e) all statutory requirements relating to the provision of accounts are complied with and all prudential reporting requirements are adhered to.
- 13 In the case of larger or more complex institutions, the Authority expects there to be a dedicated unit responsible for evaluating and monitoring all material risks within the business, including reputational and strategic risks. The operation of this unit should be subject to periodic review by internal audit.

### **Control Environment**

- 14 The strength of the internal control environment is important for licensed institutions, as weaknesses can undermine an otherwise adequate control system. 'Control environment' means the overall attitude, awareness and actions of directors and management regarding internal controls and their importance in the entity. The control environment encompasses the management style, and corporate culture and values shared by all employees.
- 15 Factors relevant to the control environment include:
- (a) the importance which is attached to controls by management;
  - (b) the way in which staff are assessed and rewarded (including remuneration and bonus schemes as well as promotion policies);
  - (c) staff training;
  - (d) the methods for reviewing control, including internal audit.

### **High Level Controls**

- 16 The Authority's requirements for adequate internal control systems apply to high level as well as to detailed control systems. High level controls are the controls which are primarily exercised at Board, director and senior manager level, as distinct from the detailed controls, the operation of which is delegated to others. High level controls typically include:
- (a) the setting of strategy and plans;
  - (b) approval of risk policies;
  - (c) establishment and review of the organisational structure;
  - (d) the system for delegation;

- (e) review of high level management information;
- (f) maintaining the framework for monitoring and/or periodic review of the detailed control system and the implementation of action points following such a review.

### **General Requirements for the Control System**

17 The Authority sees it as inappropriate to prepare a single comprehensive list of internal control procedures which would be applicable to any institution. However, internal control systems need to be adequate for the size and complexity of the business and should provide reasonable assurance that:-

- (a) the business is planned and conducted in an orderly and prudent manner in adherence to established policies;
- (b) potentially material business developments, including with regard to products or services and their delivery, or to the control environment, are reviewed and approved at Board level;
- (c) the institution's risk management strategies, policies and processes are properly documented and communicated to all those responsible for applying them and for and monitoring compliance with them; and are regularly reviewed and updated as appropriate;
- (d) transactions and commitments are entered into in accordance with management's general or specific authority;
- (e) management is able to safeguard the assets and control the liabilities of the business;
- (f) there are measures to minimise the risk of loss from irregularities, fraud and error, and to identify cases promptly when they occur;
- (g) the accounting and other records of the business provide complete, accurate and timely information;
- (h) management is able to monitor on a regular and timely basis, among other things, the adequacy of the institution's capital, liquidity, profitability and the quality of its assets;
- (i) 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;
  - (j) management is able to prepare returns made to the Authority completely and accurately in accordance with the relevant reporting instructions, and to submit them on a timely basis; and
  - (k) the institution fulfils its notification responsibilities under the Banks and Deposit Companies Act (eg Section 38 reports of large exposures).
- 18 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 proper 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.
- 19 It is the responsibility of senior 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; and it is the responsibility of the Board, through exercising appropriate oversight, to ensure that this is properly done. An independent review process in the form of an appropriate internal audit and compliance function must be in place to assist management by conducting regular reviews, designed to monitor the effectiveness and operation of the systems, to test compliance with daily procedures and controls and to manage compliance risks. This function needs both to ensure that policies and procedures are complied with and to maintain under review the adequacy and suitability of existing policies, procedures and controls for the institution's ongoing business needs.

### **Control Objectives**

- 20 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 to the nature, volume and complexity of its transactions and commitments.
- 21 It is inappropriate to provide an exhaustive and prescriptive list of detailed control requirements which should apply to all institutions. However, each institution should address the following control objectives:-
- (a) Organisational structure: Institutions should have documented the high level controls in their organisation which:
    - (i) define allocated responsibilities; and specify the delegation of authority and responsibility, together with the limits that are applicable;

- (ii) identify lines of reporting for all aspects of the enterprise's operations, including the key controls and giving outline job descriptions for key personnel.
- (b) Monitoring procedures: 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 it 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 above, and with statutory, supervisory and regulatory requirements.
- (c) Segregation of duties: 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. Risk evaluation, monitoring, control and mitigation functions must be properly segregated from the risk-taking functions within the institution, and must have independent reporting lines directly to the Board and senior management.
- (d) Authorisation and approval: All transactions should require authorisation or approval by an appropriate person and the levels of responsibility should be recorded as prescribed above.
- (e) Completeness and accuracy: 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:
  - (i) checking the arithmetical accuracy of the records,
  - (ii) checking valuations,
  - (iii) the maintenance and checking of totals,
  - (iv) reconciliations,
  - (v) control accounts and trial balances, and
  - (vi) accounting for documents.
- (f) Safeguarding assets: 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.
- (g) Personnel: 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**

- 22 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. It is the responsibility of management to understand the extent to which their institution relies on electronic information, to assess the value of that information and to establish an appropriate system of controls. The control objectives are usually 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 in a manner which is cost effective.
- 23 The types of risk 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 of an information system.
  - (c) interruption: the components of electronic systems are vulnerable to interruption and failure. Without adequate contingency arrangements, there may be serious operational difficulty and/or financial loss.
  - (d) misinformation: problems may emerge in systems that have been poorly specified or inaccurately developed. These may become immediately evident, but can also pass undetected for some time. This is a particular risk in systems where audit trails are poor and the processing of individual transactions difficult to follow.
- 24 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.

### **Money Laundering Deterrence**

25 It is a requirement of The Proceeds of Crime Act 1997 and the Proceeds of Crime (Money Laundering) Regulations 1998 [and related provisions for countering terrorist financing] that institutions have policies and procedures in place to guard against their business and the financial system being used for the purpose of money laundering. The Guidance Notes on the Prevention of Money Laundering issued from time to time by the National Anti-Money Laundering Committee provide a practical interpretation of the Regulations. They also set out the arrangements whereby institutions are required to report any suspicious activities to the police. In addition, where suspicious activities or frauds encountered by an institution may be material to the safety, soundness or reputation of the institution, the Authority should also be alerted. The Authority expects institutions to apply strict 'know your customer' rules to deter abuse and to promote high ethical and professional standards in their business. In the course of its supervision, the Authority reviews and licensed institutions' systems and controls to ensure that institutions are in compliance with their statutory obligations.

### **Outsourced Processing**

- 26 Institutions are required to record and control their business adequately. Where the processing which supports an institution's business has been outsourced, the requirements continue to apply with respect to that business.
- 27 Institutions should put in place procedures for monitoring and controlling the outsourced operations, and for ensuring that management's information requirements with respect to the outsourced operations are satisfied.

### **Internal Audit**

28 Internal audit provides independent assurance over the integrity and effectiveness of systems. All institutions must have an internal audit function. Generally, this should be located within the licensed institution itself, although it may be located elsewhere within a consolidated group, provided the Authority is satisfied as to the management and control of the process. In the case of a smaller institution, the Authority may be prepared to permit the internal audit function to take the form of appropriate independent reviews by external experts rather than by a dedicated in-house unit. The Authority views it as inappropriate

for internal audit functions to be outsourced to an external auditor, given the risk of undermining the ultimate effectiveness of the external audit process.

- 29 The scope and objectives of internal audit are dependent on 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.
- 30 The following control functions are typically undertaken by internal audit:-
- (a) review of accounting and other records and the control environment;
  - (b) assisting management with the identification of risk;
  - (c) challenging the assumptions within the control systems;
  - (d) review of the appropriateness, scope, efficiency and effectiveness of internal control systems;
  - (e) detailed testing of transactions and balances and the operation of individual internal controls to ensure that specific control objectives have been met;
  - (f) review of the implementation of management policies;
  - (g) special investigations for management where there are areas of particular concern.
- 31 It is important to ensure that the internal audit function is appropriately structured and resourced to enable it to provide an independent appraisal of internal controls. 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. Internal audit should have no authority or responsibility for the activities it audits.
- 32 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. The position of Head of Internal Audit should be a key role within the institution and, accordingly, should be undertaken by an experienced and senior individual. The objectivity and independence of internal audit must be supported by appropriate reporting lines. In most cases this would involve dual reporting lines from the Head of Internal Audit to the Chief Executive Officer or equivalent, and to the Audit Committee, usually via the Non-executive Chairman of the Audit Committee.
- 33 In reviewing the adequacy of institutions' internal audit functions the Authority has particular regard to:

- vi. the adequacy of resources, including experience and training that are appropriate to the range of business to be reviewed;
- vii. the adequacy of independence, including reporting lines, and of the ability of the function to ensure effective follow-up action;
- viii. the adequacy of access to staff, to records, files and data of the institution and affiliates (including to any outsourced functions) in so far as is relevant to the performance of the function; and
- ix. the use of a methodology, identifying all material risks, to develop suitable audit plans and to allocate resources accordingly.

### **Audit Committee**

- 34 The Authority expects all licensed institutions to have an Audit Committee with, at a minimum, two members or three in the case of a publicly listed institution. In the case of banks, the Audit Committee should comprise solely non-executive directors. In the case of deposit companies, it may be acceptable for the Committee to have a majority of non-executive directors. In all cases, the non-executives should be properly independent of the senior management of the institution. The Committee must also be chaired by a non-executive director who has suitable financial expertise or experience. The Authority will meet, normally on an annual basis, with members of institutions' Audit Committees or, as a minimum, with the Chairman of the Audit Committee.
- 35 In order for the Audit Committee to be effective:
- (a) it should have a formal constitution and terms of reference;
  - (b) the external auditors, the Head of Internal Audit and the Chief Financial Officer and/or Chief Executive Officer should normally be invited to attend meetings, at least for part of the time;
  - (c) there should be at least one meeting with the external auditors each year, without executive board members present;
  - (d) the Head of Internal Audit should have a right of direct access to the Chairman of the Audit Committee; and
  - (e) the Audit Committee should have explicit authority to investigate matters within its terms of reference and access to information and external advice.
- 36 Exceptionally, the Authority may be content for the Audit Committee of a related company also to carry out such functions in respect of a licensed institution, subject to being satisfied that that Committee will have the appropriate expertise and diligence to operate effectively.

## ANNEX D

### SECTION 39 REPORTS ON PRUDENTIAL RETURNS

1. When reporting on an institution's returns, reporting accountants are asked to carry out certain procedures to provide a level of assurance as to whether the information contained in the relevant return is completely and accurately extracted from the accounting and other records, and has been prepared in accordance with the Authority's current reporting instructions. They are not required to check and confirm that the underlying accounting and other records are themselves correct. Further, they are not normally asked to report on the systems and controls maintained to provide and control the quality of the information for the return in question.

#### **Nature of the Report**

2. The nature of the report will be an "Agreed-upon Procedures" Report. The procedures will be designed by the reporting accountants and will be agreed upon by the institution and the Authority, as users of the Report, prior to any substantive work being performed. The users of the Report will be responsible for deciding the sufficiency of the procedures for their purposes. The procedures performed will not constitute an audit and no audit assurance will be provided by it. Rather, the object is to provide a level of assurance to the Authority that the return in question:
  - a) is complete in so far as all the relevant information contained in the accounting and other records at the reporting date has been extracted and recorded in the return;
  - b) is accurate in so far as it reflects correctly information contained in, and extracted from, the accounting and other records at the reporting date;
  - c) is prepared in accordance with the current reporting instructions (including notes and definitions) and any written rulings from the Authority to the institution; and
  - d) is prepared using the same accounting policies as those applied by the institution in its most recent statutory accounts. In the event that the reporting accountants perceive any conflict between the institution's accounting policies and the Authority's specific reporting instructions, that should be identified in their report.
3. In order to perform such an examination of an institution's returns, reporting accountants should have a proper understanding of:
  - a) the returns submitted by an institution;
  - b) the Authority's current reporting instructions pertaining to the return in question;
  - c) any further rulings that have been agreed in writing by the Authority;
  - d) any policy statements by the Authority in relation to such returns.

Where the reporting accountants are in doubt about the existence of a specific ruling by the Authority or the interpretation of such a ruling, they may contact the Authority for guidance. If the point remains in doubt, this should be noted in their report.

4. In the case of returns which contain information prepared on a consolidated basis, reporting accountants may be asked to extend their procedures to the extraction of the information from the underlying records of entities within the consolidation.

### **Structure of the report**

5. The Report should provide brief details of the work conducted by the reporting accountants and set out any exceptions found during the examination, together with any qualifications relating to areas of doubt or uncertainty regarding specific rulings or interpretation of reporting instructions.
6. The report should take the following form:-

The Directors  
[ ] Limited

Reference: [ ]

Dear Sir(s)

[Unconsolidated/Consolidated] return(s) – dated [ ] (“the Return(s)”)

In accordance with your letter of instruction dated [ ], a copy of which is attached, we have performed the procedures noted below in connection with [ ] Limited's (the “Institution”) Return(s) dated [ ]. The Return(s) (is/are) the responsibility of the Institution's management.

This engagement to perform specified auditing procedures was performed in accordance with standards established by the Auditing and Assurance Standards Board of the Canadian Institute of Chartered Accountants. This report is for the sole use of management, the Board of Directors and the Bermuda Monetary Authority (BMA), who are the specified users of the report. The sufficiency of these procedures has been agreed to by the BMA as sufficient to assist them in evaluating the [unconsolidated/consolidated] Return(s) for the period ending [ ] that has been filed with the BMA. Consequently, we make no representation regarding the sufficiency of the procedures described below either for the purpose for which this report has been requested or for any other purpose.

The specified auditing procedures are as follows:

- Obtain an understanding of the process employed by the Institution in completion of the return(s)-;
- Read the return(s) and, in the context of the knowledge gained as a consequence of the work described in this report and our role as auditors of the Institution, note any inconsistencies or omissions that came to our attention as a result of reading the return(s);
- Recalculate all casts, cross-casts and cross references, where applicable;
- Agree the information on the return(s) (on a random sample basis) to the underlying accounting records and other records;
- Determine (on a random sample basis) whether information is correctly classified on the return(s) by comparing the information to underlying accounting and other records and referring to BMA guidelines and reporting instructions;
- Inspect the adjustments made to the return(s) (on a random sample basis) for accuracy, and trace each to the underlying financial records.

We attach a copy of the return(s), which we have initialed for the purpose of identification. Appendix 1 to this letter gives an outline of the systems and procedures used by the Bank in the preparation of the Return(s). Appendix 2 summarizes, for each significant balance sheet asset category, the specific procedures performed and sample sizes used.

As a result of applying the above procedures, we found [no exceptions/the exceptions set out in Appendix 3].

These specified auditing procedures do not constitute an audit of the underlying financial records or specified elements, accounts, or items included in the Return, the objective of which would be the expression of an opinion thereon. Accordingly, we do not express any such opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

This report is intended solely for the use of the specified users listed above and should not be used by those who have not agreed to the procedures and taken responsibility for the sufficiency of the procedures for their purposes.

Chartered Accountants  
Hamilton, Bermuda  
Date

## **Annex E**

### **AUDITORS' REVIEW OF INTERIM PROFITS**

The Report should take the following form:-

To the directors of Institution ABC Ltd

We have reviewed the balance sheet of ABC Ltd as at [date] and the statements of income, retained earnings and cash flows for the [three/six month] period then ended. These financial statements are the responsibility of the management of the company.

We conducted our review in accordance with standards established by [The Canadian Institute of Chartered Accountants] for a review of interim financial statements by an entity's auditors. Such a review consists principally of applying analytical procedures to the financial data, and making enquiries of, and conducting discussion with, persons responsible for financial and accounting matters. A review is substantially less in scope than an audit, the objective of which is the expression of an opinion regarding the financial statements; accordingly, we do not express such an opinion. A review does not provide reassurance that we would become aware of any or all significant matters that might be identified in an audit.

ABC Ltd results for the period ended [date] have been issued to the shareholders in the form of a report. This report does not include certain items that are required to be separately presented and certain disclosures that are required to be made in the accompanying footnotes under [Canadian] generally accepted accounting principles.

Based on our review, and except as noted in the preceding paragraph, we are not aware of any material modification that needs to be made for these financial statements to be presented fairly in accordance with [Canadian] generally accepted accounting principles.

This report is solely for the information and use of the Board of Directors of ABC Ltd and the Bermuda Monetary Authority and is not intended for, and should not be used by, anyone other than these specified parties.

Chartered Accountants  
Hamilton, Bermuda  
Date