Objective

- To emphasize and strengthen the quality and effectiveness of the internal audit function.
- To re-emphasize the role, duties and responsibilities of internal auditors to the Board of directors (Board), all levels of management and external auditors.
- To provide a uniform practice on internal auditing which would serve as a basis for guidance and measurement of the performance of internal audit function.

Scope

- Applicable to all licensed commercial banks, merchant banks / investment banks, insurance companies and their subsidiaries. Where applicable, Islamic Banks, Takaful companies and their subsidiaries should adhere to the Guidelines.
- It is also applicable to the internal audit function of the financial institutions which is undertaken by the institution’s group internal auditor.
- The guidelines should be read in conjunction with the Guidelines on Corporate Governance for Licensed Institutions and guidelines previously issued by the former Jabatan Pengawalan Insurans (JPI) and guidelines issued by Jabatan Dasar Kewangan Pruden from time to time on audit committee (AC) for insurance companies.
- The Guidelines, however, only serve as a general guide for the internal auditors of financial institutions and not intended to provide comprehensive guide of all possible situations that the internal auditor may encounter in the course of audit. The Guidelines are also not meant to be exhaustive nor intended to provide detailed audit steps required to perform the audit of every operational area of financial institutions.
- The internal auditors should also be guided by the authoritative pronouncements issued by the relevant professional accounting and auditing bodies.

Rationale

- Bank Negara Malaysia examinations of financial institutions continue to disclose the discrepancy in the standard of internal audit function among the financial institutions, hence the principle behind the issuance of the Guidelines. The internal auditors also need to assess the effectiveness of corporate governance, operational efficiency and productivity, asset quality and other inherent operating and financial risks. Information systems (IS) audit function should also be enhanced to keep up with the rapid computerisation of the operations of the banking and insurance sectors.
- In addition to carrying out their traditional role as the financial intermediaries, a financial institution's role has become more complex and with the continuing pressure to operate profitably, the industry has adopted innovative business approaches. This includes the management of complex assets and liabilities, search for additional sources of income, reaction to technological advances, response to changes in regulatory policy, and competition for deposits and insurance premiums have all added to the risks and complexities of the businesses of the financial institutions. As a result, the innovation and complexity of the industry's pursuit of profitable activities create a constantly changing body of business and economic risks. These factors, together with the rapid pace of expansion in branch network, the increasing sophistication of operations and the centralisation of operations at the head office or regional processing centres, call for a more dynamic rather than static audit process. Towards this end, internal auditors are expected to play a greater and more proactive role in carrying out management and compliance audits and to assist the financial institutions to achieve their objectives and goals.
- The importance of internal audit function to a financial institution needs to be re-emphasised. An effective internal audit function should serve as a resource to the management. The internal auditors should not only assess the soundness and adequacy of internal controls but also determine whether the established policies and procedures are effective in practice. The internal auditors should be able to advise management on

the adequacy and effectiveness of the policies and procedures in protecting the organisation against the attendant new risks.

PART I: ORGANISATION OF INTERNAL AUDIT FUNCTION

1. OVERVIEW

1.1. Internal auditors play an important role in helping to establish and maintain the best possible internal control environment at their financial institutions. An effective internal audit function is crucial to ensure a sound financial system as a whole. Important consideration has to be given to the organisation of the internal audit function in the financial institution to ensure its effectiveness. The issuance of Bank Negara Malaysia guidelines on AC and internal audit departments have paved the way to independence and objectivity of the internal audit function, fundamental among them is the requirement for the establishment of an AC. Besides independence and objectivity, professional proficiency and integrity are key characteristics expected of internal auditors.

1.2. Certain financial institutions, which by virtue of their nature and size of operations may find the establishment of an internal audit department too onerous. For reasons of synergy and economies of scale, the financial institutions may use the services of the group internal auditors. Under such circumstances, the reporting lines of the internal audit function must be clearly defined. However, before the group internal audit department can render its services to the licensed institutions as defined in the Banking and Financial Institutions Act 1989 (BAFIA), they need to get approval from Bank Negara Malaysia. This Part explains the minimum requirements expected of the internal audit function of all financial institutions with regard to the independence and objectivity, professional proficiency, relationship and communication and audit governance.

2. AUDIT COMMITTEE

An AC generally consists of non-executive directors. As stipulated in the guidelines, the role of the audit committee is basically to provide avenue for the internal audit department to effectively voice their findings. The effectiveness, independence and how influential the audit committee is, would to a great extent, depend upon the professional competence of the members themselves. The composition, authority, duties and responsibilities of the audit committee are stipulated in the Guidelines on Corporate Governance for Licensed Institutions and guidelines previously issued by the former Jabatan Pengawalan Insurans (JPI) and guidelines issued by Jabatan Dasar Kewangan Pruden from time to time on audit committee (AC) for insurance companies. Any references to the AC in the Guidelines should be read in conjunction with the above guidelines.

3. INDEPENDENCE AND OBJECTIVITY

In order to deliver impartial and unbiased judgement for the proper conduct of audits, the important prerequisites for the internal auditors is their objectivity and independence. Internal auditors should not only be independent in fact but also be seen to be independent.

3.1 Organisational Status

3.1.1 To allow the internal auditors to accomplish their audit objectives, the status of the internal audit department within the financial institutions overall organisation structure should be sufficient and distinct. Internal auditors should have the support of the management in order to gain the cooperation of the auditee and to perform their work free from interference. The position of the Chief Internal Auditor (CIA) should be equivalent to the status of other key functional heads to enable him to deal effectively with his peers and superiors when discharging his duties and responsibilities. The appointment, remuneration, performance appraisal, transfer and dismissal of the CIA should be decided by the AC.

3.1.2 The CIA should be functionally responsible to the AC although administratively, he may report to the Chief Executive Officer (CEO). The CIA should have unrestricted access to the AC. Regular communication with the AC helps to assure independence and provides the means for the CIA to keep the AC informed on audit matters.

3.1.3 Internal auditors should not be responsible for any operational or system function. Internal auditors should have unrestricted access to the institution's records, assets, personnel and premises which are essential to them so that they can have a proper conduct of the audit. If there is any restriction, it should be promptly communicated in writing to the AC for the latter to resolve with the management.

3.2 Objectivity

3.2.1 Objectivity is an independent mental attitude which would enable the internal auditors to exercise judgement, express opinions and present recommendations with impartiality.

3.2.2 The internal auditors should at least observe the following:

(a) Avoid any conflict of interest situation arising either from their professional or personal relationships in an organisation or activity which is subject to audit;

(b) Have no authority or responsibility over any unit or activity that is being audited;

(c) Should not be assigned to audit operational areas which they were previously involved in as non-audit staff until an independent audit has been conducted during the intervening period; and

(d) Act in advisory capacity when recommending controls on new systems or reviewing procedures and products prior to their implementation.

4. PROFESSIONAL PROFICIENCY

The quality, training and experience of the audit staff substantially determine the effectiveness of audit. In order to ensure the internal audit staff to be suitably qualified, they should be provided with the necessary training and continuing professional education. This is done for the purpose of enhancing or enriching their audit and technical skills.

4.1 Resources

The CIA, in consultation with the CEO, has to decide the right resources required for the internal audit department taking into consideration the size and complexity of operations of the financial institutions. The level of the resources required should be justified and endorsed by the AC. The CIA should set up suitable criteria for the recruitment of the internal audit staff. The effectiveness of the internal audit function may be enhanced by the use of specialist staff or consultants, particularly when the auditable areas are highly technical in nature.

4.2 Qualification, Knowledge, Experience and Skills

4.2.1 The academic background and expertise required of the CIA varies depending on the size and complexity of the financial institution's operations and on the management's emphasis placed on the internal audit function. Essentially, to commensurate with his position in the organisational hierarchy, the CIA should possess relevant academic/professional qualification and sufficient audit experience. However, those without the relevant academic/professional qualification but regarded by management to be competent may also be considered for the post of CIA. The CIA should also have indepth knowledge of the business and organisational, technical, communication and other relevant skills.

4.2.2 Internal auditors should be proficient in applying approved auditing guidelines and accounting standards, legal and regulatory requirements, directives and guidelines issued by Bank Negara Malaysia and other authorities, and other rules and regulations issued by the relevant associations of the banking and insurance industry.

4.3 Supervision

Supervision is a continuing process from planning the audit to the conclusion of the audit assignment. The CIA is responsible for the audit performance by his subordinates. The CIA should ensure that the audit objectives stated in the approved audit programme have been achieved. The CIA should set a reasonable time frame for the completion of each audit assignment (that is, from the commencement of the assignment to the issuance of the audit report) after considering its nature and complexity.

4.4. Code of Ethics

The internal auditors should at all times exercise due professional care when discharging their duties and responsibilities. They should carry out their work independently, objectively, professionally and with utmost good faith. The internal auditors should avoid any conflict of interest situation and subject themselves to the highest ethical standards. They have the obligation to maintain strict confidentiality with regard to all information obtained in the course of their work and must never misuse any privileged information for personal gain. Internal auditors should comply with Bank Negara Malaysia guidelines, relevant laws and regulations and the requirements of relevant professional bodies.

4.5 Training

It is the responsibility of the AC to ensure that the internal audit staff have been given necessary training to perform the audit work. There should be a programme of continuing education and training to enable the internal auditors to keep abreast with industry developments and enhance their technical skills. The CIA should ensure that on-the-job training is to be provided to the new recruits under the supervision of suitably competent and experienced internal auditors. Training should be a planned and continuous process for all levels of internal audit staff. The CIA, in consultation with the AC and the CEO, should determine the budget requirements for the training needs of the internal audit department.

5. RELATIONSHIP AND COMMUNICATION

Internal auditors are expected to have constructive working relationship with the management and should be in constant communication with the external auditors and Bank Negara Malaysia on areas of common interest.

5.1 Management

There should be mutual respect and collaboration between the management and internal auditors. Consultation with management may lead to the identification of areas of audit concern which require the ClA's attention. Internal auditors should avail their expertise in an advisory capacity as a value-added resource to the management.

5.2 External Auditors

Internal auditors should liaise closely with the external auditors in the planning and execution of the reviews on internal controls. In addition, regular meetings should be held with the external auditors on areas of common concern such as audit planning, audit priorities and scope to avoid overlapping of work.

5.3 Bank Negara Malaysia and Other Regulatory Authorities

5.3.1 Internal auditors should immediately report to the AC and CEO any significant audit findings uncovered in the course of audit that would adversely affect the financial institution's operation and financial condition. Bank Negara Malaysia should be promptly informed of such audit findings. The CIA should monitor all corrective actions taken by the management with regard to Bank Negara Malaysia examination findings and report to Bank Negara Malaysia any instances where corrective actions have not been taken.

5.3.2 Internal auditors should maintain close cooperation with other regulatory authorities on areas of common interest.

6. AUDIT GOVERNANCE

Internal audit department should have an audit charter, an audit plan, audit manual, audit programme and internal control questionnaires (ICQ) in place. Although these documents may be called by different names and differ in comprehensiveness, they are accepted as long as they serve the intended purpose.

6.1 Audit Charter

The audit charter is a formal written document that identifies the purpose, authority, scope, independence and responsibility of the internal audit function. The audit charter must be approved by the audit committee and endorsed by the Board so that the internal audit function may be effectively discharged. Additionally, the audit charter serves as a platform to inform the CEO and all levels of management on the role, duties and responsibilities of internal auditors.

6.2 Audit Plan

The CIA should develop an audit plan as a means of directing and controlling the audit work. The audit strategic plan may range from one to five years depending on the size and complexity of operations. The plan should set out the audit objectives, auditable areas, scope of coverage, frequency of audit, resources required and duration of each audit assignment. The CIA should assess the risks of the auditable areas before determining the audit frequency and scope of coverage. The risk assessment methodology used for this purpose should be documented and regularly reviewed. As a general guide, audit cycle for all auditable areas should be at least once a year. However, the CIA has the discretion to determine the audit cycle for auditable areas deemed not critical if the financial institution has an effective risk assessment system in place. The CIA should also include management audit in the audit plan. The audit plan must be endorsed by the AC and should be flexible to respond to changing priorities or needs.

6.3 Manual

The audit manual provides the audit department personnel with a set of uniform audit standards for guidance and reference. It also serves as a valuable training aid for new recruits. The audit manual should contain written audit policies, objectives, standard procedures and programmes. The CIA should ensure that the audit manual is comprehensive enough to cover at least the major operations of the financial institution and is modified periodically to reflect corporate, regulatory and industry trends.

6.4 Audit Programme and Internal Control Questionnaires (ICQ)

Audit programme is a set of detailed step-by-step audit procedures for each auditable area and is usually supplemented by the ICQ. Both the audit programme and ICQ should be comprehensive and tailored to keep abreast with the current developments relevant to the industry. A well-designed audit programme and ICQ would provide a systematic audit approach. In addition, the internal auditors' judgement and analytical skills are essential in ensuring high quality audit.

PART II DUTIES AND RESPONSIBILITIES

1. OVERVIEW

The core function of an internal audit department is to perform an independent appraisal of the financial institution's activities as a service to the management. The internal audit function plays an important role in helping management to establish and maintain the best possible internal control environment within the financial institution. A sound internal control environment would ensure the financial institution's compliance with legal and regulatory requirements, safeguarding of assets, adequacy of records, prevention or early detection of frauds, material errors and irregularities and efficiency of operation. This Part describes the main duties and responsibilities of the internal auditors which are necessary in promoting a sound financial system.

2. ADEQUACY AND EFFECTIVENESS OF SYSTEM OF INTERNAL CONTROL

It is the responsibility of the internal auditor to ensure the soundness and adequacy of the financial institution's accounting and operating controls. Careful evaluation of the system of internal control should be made to assess the degree of reliance the management can place on these controls. The internal auditors should determine whether the established system of internal control is effective, operative and complied with. The review of the system of internal control should be made ongoing to ensure that internal control continue to effectively support the successful execution of the financial institution's business strategies. The reliability and integrity of financial information and the means used to identify, measure, classify and report such information also need to be assessed to ensure sound management information systems (MIS).

3. COMPLIANCE WITH POLICIES, PROCEDURES, RULES, GUIDELINES, DIRECTIVES, LAWS AND REGULATIONS

In the process of carrying out their audit, the internal auditors should evaluate whether the financial institution is in compliance with the applicable laws and regulations, guidelines and directives issued by Bank Negara Malaysia and other regulatory authorities, and applicable rules set by the various associations. The internal auditors should also review compliance with the internal policies and procedures of the financial institution.

4. DETECTION OF FRAUDS, ERRORS, OMISSIONS AND OTHER IRREGULARITIES

Management has the responsibility to prevent and detect earlier the signal for frauds, errors, omissions and other irregularities through the implementation and continued operation of an adequate system of internal control. Hence, such a system reduces but does not eliminate the occurrence of frauds, errors, omissions and other irregularities. In assessing the soundness and adequacy of the system of internal control, the internal auditors should ensure that they are always alert especially when there are circumstances shown that the internal control environment in the financial institution is weak or conducive for the perpetration of fraud or increases the risk of fraud or error.

5. MANAGEMENT AUDIT

The internal auditors should review to ensure that the available resources are deployed and utilized in the most efficient, effective and economical way so as to provide value-added services to the management. This is to determine whether management has established adequate systems and suitable procedures to ensure the accomplishment of the financial institution's objectives and goals.

6. INFORMATION SYSTEMS AUDIT

The computerisation of financial institution's operations has changed the work procedures, processing of information and maintenance of records. Internal auditors should ascertain that adequate controls are in place to minimise the vulnerability of information and to provide the necessary protection against the possibility of frauds and errors. Generally, an important aspect of the financial institution's internal control structure is the computerisation of operations. Therefore, it is crucial for the internal auditors to carry out information system audit in order to ascertain that control features are adequate to cover all computerised activities and effective to support the financial institution's operation and reporting requirements.

7. PARTICIPATIVE AND CONSULTATIVE ROLE

7.1 In order to assist the management to accomplish the financial institution's overall objectives and goals, it is imperative that the internal auditors play a participative and consultative role. As the activities of the financial institutions have become increasingly diverse and complex and coupled with the competitive environment, internal auditors may be requested to participate on a consultative basis in the development of new products and systems to ensure that the necessary control features are incorporated. However, the internal auditors' consultative role should be made known to the management in order not to be construed as compromising their independence.

7.2 To provide value-added services to the management, the internal auditors' expertise may be consulted in the planning, design, development, implementation and operation of major computer-based systems. The internal auditors should participate in this role in an advisory capacity.

PART III SCOPE OF AUDIT WORK

1. OVERVIEW

1.1 Generally, audit scope should entail the examination and evaluation of all functions and activities of the financial institutions including control features, operational systems and procedures as well as assessment of the quality of management performance in discharging their duties and responsibilities. This Part deals with the scope of audit which the internal auditors are required to perform when carrying out an audit assignment. The minimum audit coverage on the specific critical areas of operations is discussed in Part V of the Guidelines.

1.2 The scope of audit work covered under this Part should not be construed to be exhaustive but serves to provide the minimum scope to be covered under any audit assignment. The CIA should ensure that sufficient coverage and depth be given to each audit assignment based on the assigned risk factors. The CIA, after having considered the level of risk for each auditable area, should decide whether to expand or limit the audit scope. Such decision should be properly documented. The internal auditors should also decide on the appropriate level of audit sampling in order to achieve their audit objectives. The internal auditors should be guided by the International Auditing Guideline on Audit Sampling.

2. EVALUATION AND APPRAISAL OF SYSTEM OF INTERNAL CONTROL

It is the responsibility of the management to establish a strong system of internal control in order to ensure the soundness of financial institutions. An effective system of internal control helps to reduce the risk of frauds, errors, omissions and other irregularities from occurring. In a computerised environment or otherwise, the internal auditors should understand, document, evaluate and test the system of internal control. The audit scope should cover the effectiveness of the system of internal control, the reliability and integrity of MIS, the prevention or timely detection of frauds, errors, omissions and other irregularities, and the means for the safeguarding of assets. The areas of audit concern are discussed below:

2.1 Effectiveness of System of Internal Control

The effectiveness of system of internal control depends, among others, on the overall control environment in which the financial institution operates. However, a strong control environment does not by itself ensure the overall effectiveness of the system of internal control. As a result, the internal auditors have to be wary of other factors that may affect the control environment. For each auditee, the extent of audit coverage and frequency would depend on the assigned risk factor of the auditee based on a risk assessment methodology applied during the audit planning. When the assigned risk level of the auditee is high, the scope of the audit should be expanded to compensate the risk. The internal auditors have to be satisfied that the overall system of internal control is effective, adequate and functioning as planned; key control procedures exist and are adhered to; proper segregation of incompatible functions is practised at all times; and the existing control systems are adequate in realising the financial institutions objectives and goals.

2.2 Reliability and Integrity of Information

Internal auditors should review the relevance, reliability and integrity of financial and operating information generated and the means used to identify, measure, classify and report such information. In addition, internal auditors should determine that information is provided to the management on a timely basis for their decision making. For each audit concern, the internal auditors should perform the following:

(a) Ensure that financial and operating records and reports contain accurate, reliable, timely, complete and relevant information and are prepared in compliance with approved accounting standards;

(b) Determine that control procedures over record keeping and reporting are adequate and effective;

(c) Evaluate the process in which information is captured, recorded and protected;

(d) Ascertain that the system for generating reports to Bank Negara Malaysia is adequate and effective; and

(e) Verify accounting records and reconciliations.

2.3 Safeguarding of Assets

To safeguard the financial institution's asset against losses from theft, fire and unauthorised use, the internal auditors should review whether there are adequate controls in place. Assets in this context cover all physical assets beneficially owned by the financial institution.

2.4 Detection of Frauds, Errors, Omissions and Other Irregularities

2.4.1 The existence of an effective system of internal control reduces but does not eliminate frauds, errors, omissions and other irregularities from occurring. There will always be some risk of internal controls failing to operate as planned. Fraud involving collusion among employees or fraud committed by the management will lead the system of internal control to be ineffective. Although internal auditors are not responsible for detecting frauds, errors, omissions and other irregularities, they should be vigilant and alert where auditee's operations substantially deal with cash transactions or involve high risk activities.

2.4.2 The internal auditors should be in a position to determine the auditable areas where the possibility of frauds, errors, omissions and other irregularities are most likely to occur. Accordingly, the audit scope should be widened to cover at least the following areas of concern:

(a) The system of internal control is deemed to be effective when such errors and omissions (whether intentional or unintentional and irrespective of their materiality) are prevented or detected promptly;

(b) The errors, omissions or defalcations can be concealed especially in situations where the persons holding those positions have the access to the asset and are able to manipulate the records;

(c) Major deviations from established policies, practices and procedures are investigated;

(d) When the propriety of management's claims is ascertained, then, the claims incurred must be in line with the financial institution's approved policies and procedures; and

(e) Indicators exist whereby records can be manipulated especially when key officers or other employees' financial rewards are linked directly to the operating results.

2.4.3 During the course of the audit, if significant control weaknesses are uncovered or internal auditors have received information from sources within or outside the organisation about suspicious activities, the internal auditors' scope should be extended to confirm or dispel whether frauds, errors, omissions and other irregularities have occurred. An investigation is warranted if there is sufficient evidence or indication that fraud or material irregularities are likely to occur. The results from the investigation should be informed to the management and Bank Negara Malaysia. A police report should be made, if necessary, when criminal wrongdoing is suspected. The internal auditors should assist management to revise and strengthen the control features to prevent the recurrence of similar fraud or material irregularities in the future.

3. COMPLIANCE WITH POLICIES, PROCEDURES, RULES, GUIDELINES, DIRECTIVES, LAWS AND REGULATIONS

All financial institutions should ensure strict compliance with all applicable laws and regulations, guidelines, directives, reporting requirements and internal policies and operating procedures. The audit scope should cover the financial institution's compliance with:

(a) The BAFIA, the Islamic Banking Act 1983, the Exchange Control Act 1953 and the Exchange Control Notices, the Insurance Act 1996 and the Insurance Regulations, the Takaful Act 1984 and other applicable laws and regulations;

(b) Guidelines, directives and circular issued by Bank Negara Malaysia and pronouncements or rules issued by the relevant associations; and

(c) Internally approved policies and operational procedures.

4. ADEQUACY AND EFFECTIVENESS OF RISK MANAGEMENT SYSTEM

4.1 A risk management system is essential to the financial institution. Therefore, management should develop a formalised system to ensure that risk exposures are identified and adequately measured, monitored and controlled that is in line with the increasing competition, complexities of operations and financial innovations. The risk management system should commensurate with the scope, size and complexity of the financial institution's activities and the level of risk a financial institution is prepared to assume.

4.2 Overall, all the financial institutions, particularly the commercial banks which are engaged in the financial derivative activities, should have a comprehensive risk management system. Therefore, the process of risk management for derivative activities should be integrated with the financial institution's overall risk management system to the fullest extent using a conceptual framework common to the financial institution's other activities. Such a common framework enables the institution to manage its consolidated risk exposure more effectively.

4.3 While the minimum audit coverage to be performed on derivative activities is covered in Part V of the Guidelines, the following are the audit concerns with respect to the overall risk management system:

(a) Effective management supervision is practised by the Board and its delegated authorities;

(b) Procedures that identify and quantify the level of risk on a timely basis are in place;

(c) Limits or other controls are in place to manage the risk;

(d) Reports to the management accurately present the nature and level of risk taken and any non-compliance with approved policies and limits;

(e) Responsibilities for managing individual risks are clearly identified; and

(f) Procedures relating to the calculation and allocation of capital to risks are in place.

4.4 Internal auditors should design auditing procedures that would assess the integrity of risk measurement, adequacy of control and reporting systems and compliance with approved policies and procedures.

5. ECONOMICAL, EFFECTIVE AND EFFICIENT USE OF RESOURCES

5.1 The principal objective of any financial institutions is to increase its profitability through the economical, effective and efficient use of available resources. It is the responsibility of the management to set the measurement standards, benchmarks or productivity indices to gauge the returns from the utilisation of these resources. And these measurement standards, benchmarks or indices have to be approved by the Board.

5.2 The internal auditor should play a proactive role to determine the financial institution’s optimum utilisation of available resources that lead to the accomplishment of the organisation’s overall objectives and goals. Such role will add value to their service to the management. Hence, the internal auditors should extend its traditional role of compliance audit to cover management auditing.

5.3 With regard to management audit, the internal auditors should review whether:

(a) Established system for planning, appraising, authorising and controlling the use of resources are operational and effective;

(b) Operating standards have been established for measuring the economy, efficiency and effectiveness of resources employed and have been met;

(c) Deviations from operating standards are promptly identified, analysed and communicated to those responsible for taking remedial measures; and

(d) Remedial or corrective actions have been taken.

5.4 In performing management audit, the internal auditors should highlight to the management whether there are underutilised resources, non-productive work, procedures which are not cost justified and over or understaffing. Internal auditors should ensure that management has developed action plans to address these deficiencies. Follow-up audit should be conducted to ascertain that the action plans have been implemented.

6. ACCOMPLISHMENT OF ESTABLISHED OBJECTIVES AND GOALS

6.1 The Board is responsible for the business plan and strategy to achieve the financial institution's overall objectives and goals. Based on the objectives and goals set by the Board, the management is responsible for establishing operating or programme objectives and goals, developing and implementing control procedures, and accomplishing the desired operating or programmed results.

6.2 In evaluating the accomplishment of established objectives and goals, the internal auditors' scope should cover the entire operations or a subsection of it to determine whether:

(a) Objectives and goals are clearly set and measurable;

(b) Objectives and goals have been articulated and communicated to all staff and are being met;

(c) Adequate controls are established for measuring and reporting the accomplishment of objectives and goals;

(d) An effective control mechanism is implemented to monitor actual performance against budget. Any significant variances are analysed, investigated and promptly reported to the management and the Board;

(e) Management has considered the strengths, weaknesses opportunities and threats of the respective operation or ` programme;

(f) The achievement of established objectives and goals is in compliance with policies, plans, procedures, laws and regulations; and

(g) The underlying assumptions used by management in developing business plan and strategy are appropriate and reasonable.

PART IV REPORTING AND DOCUMENTATION

1. OVERVIEW

1.1 Internal audit reports provide a formal means of communicating audit results and recommended actions to the management and the AC. Audit reports provide the basis for the AC to highlight significant weaknesses and the management's proposed remedial measures to the Board. The management's acceptance of the internal auditors' recommendations is for reducing risks, strengthening internal controls and correcting errors would be the desired result of the audit reports.

1.2 It is of primary importance that in the course of the audit, should the internal auditors uncover major findings or frauds that would significantly affect the financial institution’s financial position or operations, they should immediately inform the management to ensure prompt corrective actions are taken.

2. AUDIT REPORT

2.1 At the end of each audit assignment, a signed report should be issued irrespective of the significance of the issues raised. The internal auditors should discuss the audit results and the recommendations thereof with the auditee before the final audit report is issued. The discussion should be carried out with those individuals who are knowledgeable of detailed operations and those who can authorise the implementation of corrective actions. The comments from the management of the auditee should preferably be incorporated in the final audit report. The CIA should review and approve the final audit report before it is presented to the AC. A copy of the final audit report should be forwarded to the AC, the auditee, the CEO and Bank Negara Malaysia on a timely basis.

2.2 Where the completion of an audit is likely to take a longer period, interim audit report may be issued to communicate any significant issues which require management's immediate attention. The AC and the CEO should be kept informed regarding the issues as well as the audit progress. The issuance of interim audit report does not diminish or eliminate the need for the internal auditors to prepare a final report. The discretion as to whether an interim audit report is warranted rests with the CIA.

2.3 The CIA should ensure that an audit report should be of sufficient quality so as to command management's attention. In order to communicate the audit results effectively, the following standards should be adopted:

(a) Audit report should be objective, clear, concise, constructive and timely;

(b) The structure of the audit report should preferably include the following:

(i) An executive summary;
(ii) Date of report and period covered by audit;
(iii) The scope and objectives of the audit;
(iv) The significance and magnitude of the problems or issues;
(v) The causes of the problems or issues;
(vi) Recommended solutions or preventive actions;
(vii) Auditee's comments on the issues and recommendations, and remedial measures taken or proposed to be taken to address the audit issues;
(viii) Management's achievements noted during the audit; and
(ix) Overall conclusion.

3. ACTION AND FOLLOW-UP ON AUDIT RECOMMENDATIONS

3.1 Management should treat all audit findings and recommendations seriously. Management's response to the audit findings should preferably be included in the report. The internal auditors should monitor whether corrective actions have been carried out on internal audit findings and recommendations, unless management has understood and assumed the risk of not taking action.

3.2 Management's plan of corrective actions and implementation time table for completion should be developed and jointly agreed upon between the management and the auditee. The status of the corrective actions should be monitored and reported to the audit committee and the CEO so that follow-up action can be taken to inform the appropriate levels of management on outstanding audit issues.

4. REPORTING OF SIGNIFICANT FINDINGS AND FRAUDS

4.1 The internal auditors should immediately report to the AC and the CEO any significant of the audit findings uncovered in the course of audit that would adversely impact the financial institution's operating and financial condition. BNM should also be promptly informed of such findings. Significant financial findings are those that would have an adverse impact on the financial performance and condition of the financial institutions. Significant non-financial findings represent fundamental weaknesses that could lead to the collapse of the financial institution's system of internal control. The immediate audit report should incorporate preliminary summary findings, the impact or potential impact on the financial position and operations of the financial institutions, and the proposed actions to be carried out by the internal auditors to investigate the matters.

4.2 Once the investigation is completed, a detailed report should be submitted to the AC, the CEO and Bank Negara Malaysia. The investigation report should be as comprehensive as the normal detailed audit report outlined in paragraph 2.3 above. It may also provide progress report on the management's continuous actions to address the weaknesses and measures taken to prevent or minimise their recurrence.

5. CONTROL AND FILING OF AUDIT REPORTS AND WORKING PAPERS

The internal audit reports and working papers should be treated confidentially. The internal audit reports should only be disclosed to those persons authorised by the AC. The internal audit working papers should be properly filed and stored, as the internal audit working papers provide evidence of audit coverage and documentation of audit trails. Other than that, to ensure systematic filing and control of audit reports and working papers, the following minimum procedures should be observed: -

(a) The format for the working papers should be standardised;

(b) There should be adequate referencing to identify the audit records, files and working papers created; and

(c) There should be a system for filing and retrieving past reports and working papers.

6. RETENTION OF AUDIT REPORTS AND WORKING PAPERS

As a minimum requirement, the audit working papers from routine audits should be retained until the next audit is carried out on the same auditable area. Reports and working papers on investigation matters should be retained for at least seven years or such period until the matter is closed. However, all the internal audit reports should be retained for at least three years or until the next audit report on the same auditable area is completed.

PART V AUDIT OF CRITICAL AREAS OF OPERATIONS

1. OVERVIEW

1.1 Part I to Part IV address the minimum requirements expected of the internal audit function of the financial institutions and would provide the foundation for a strong and effective internal audit function. Internal auditors are expected to review all auditable areas of the financial institutions. However, internal auditors should focus their attention and direct their available resources to those operations or units which cause significant risks that may have an adverse impact on the operations and financial condition of the financial institutions.

1.2 Part V covers the auditable areas a financial institution's operations that are deemed to be critical and the minimum scope of audit work which the internal auditors must perform in the course of audit. The critical operational areas identified are Credit Operations, Treasury Operations, Derivatives, Investment in Debt and Equity Securities, Information Systems, Insurance Underwriting and Insurance Claims. These critical areas of operations are not meant to be exhaustive and the internal auditors should also identify and review other operational areas deemed to be critical to the specific business undertaken by the financial institutions.

1.3 In reviewing the critical areas of the operations, it is vital to ensure the audit coverage is comprehensive. If there is a serious unsatisfactory feature that is uncovered in the course of audit, then the internal auditors should extend their scope of findings.

2. CREDIT OPERATIONS

2.1 Introduction

Credit operations involve credit appraisal, approval, documentation, disbursement, supervision, recovery and rehabilitation. Credit operations cover the extension of both on and off-balance sheet credit facilities. In most banking institutions, loans and advances usually account for a significant proportion of the assets and contribute a substantial portion of total revenue. The risks associated with the credit operations are crucial and have to be addressed and managed. The banking institution's credit strategy, policies and risk management would affect the quality of loans and advances. Subsequently, this could have a major impact on the profitability, liquidity and solvency of the banking institutions.

2.2 Credit Strategy

A banking institution's credit strategy includes the organisation's defined objectives and goals for the extension of credit facilities so as to achieve profitable returns while managing risks within the credit portfolio. The credit strategy should establish a fundamental market posture, set goals for portfolio growth or contraction, impose limits on industry and geographical concentrations, formulate policies on interest rates, margin and fees, and identify and manage risks. The management usually determines the credit strategy and subsequently it will be approved by the Board. Management should regularly review the credit strategy and policies to keep pace with the competition and changing market and economic conditions. The banking institution should address the risks inherent in credit operations when developing its credit strategy.

2.3 Risks Inherent in Credit Operations

2.3.1 The most significant risk involved in credit operations is the credit risk of a borrower. The potential inability of the borrowers to meet their repayment obligations will have an adverse impact on the banking institution's profitability, liquidity and solvency. The borrowers' repayment capacities may be affected by various factors, such as general economic condition, level of interest rates, unemployment and downturn in particular economic sectors and markets. As such, it is essential for the management to have risk grading system on the borrowers. The internal auditors should assess whether the banking institutions have adequately dealt with the potential credit risk profile of the borrowers in its credit policies and procedures.

2.3.2 Other risks that are associated with credit operations include collateral, concentration, country, foreign exchange, fraud, prepayment, interest rate, legal and regulatory, management and operational risk.

2.4 Policies and Procedures

2.4.1 It is the responsibility of the management to establish sound and prudent policies and procedures. These credit policies and procedures may be in the form of credit manuals, credit standards or guidelines. The credit policies, which should be formalised and approved by the Board, generally set the direction of lending, approving limits, credit concentration, credit criteria for prospective borrowers, types of acceptable securities, security documentation and prohibited lending. Usually, the credit procedures will outline the detailed guidelines on the various credit processes and credit administration, including among others, monitoring and classification of delinquent credit, loan write-off and reporting. Thus, the Board will delegate the authority to set the credit policies to the management committee.

2.4.2 Based on the risk management methodology, the CIA should decide on the scope of audit coverage. In any cases, all large credit exposures granted to individual borrowers or a single group of borrowers must be reviewed. The internal auditors should address the following areas of audit concerns:-

(a) Credit policies and procedures are adequate;

(b) Credit operations are in line with the approved credit strategy, policies and procedures;

(c) Proper segregation of duties and responsibilities relating to loan processing, approval, custody of security and legal documents and loan administration is practised;

(d) Creditworthiness and repayment capacity of the borrowers are carefully appraised and evaluated prior to the approvals of credit facilities;

(e) Credit disbursement are only made after the security and legal documentation have been duly completed;

(f) Effective systems are in place for credit monitoring, supervision and recovery, accounting and financial reporting;

(g) No over concentration of credit to a particular economic sector at institutional level;

(h) Management review of credit exposures to borrowers is carried out periodically and in a timely manner;

(i) No credit facilities are granted for self-serving purposes that is, credit facilities to nominees of the directors and officers of the banking institutions; and

(j) Loan documents and correspondences are properly maintained.

2.5 Security and Legal Documentation

2.5.1 If the banking institution's interest in the credit exposures is not legally protected, they may be exposed to credit loss. It is pertinent that security and loan documents are duly executed, validated and lodged with the relevant authority (for example, the Registrar of Companies and Land Office) before the borrowers are allowed to utilised the credit facilities. Most banking institutions have their own panel of solicitors and professional valuers to assist in the security and legal documentation and the appraisal of landed securities. The procedures pertaining to the safe custody of the security and legal documents must be properly addressed by the management to ensure that there is adequate segregation of incompatible functions.

2.5.2 In carrying out the checking and physical verification of the security and loan documents, the internal auditors should pay particular attention to the following audit aspects:

(a) Banking institution's legal beneficiary rights to collateral have been duly registered with the authorities to ensure its enforceability in the event of borrowers' defaults;

(b) Ensure the procedures relating to the safekeeping of and control over the access to security documents and proper maintenance of collateral records are adequate;

(c) Security and loan documentation are undertaken by the banking institution's panel of solicitors or other approved solicitors;

(d) Appraisal of value of landed security are undertaken by the banking institution's panel of valuers or approved valuers; and

(e) Procedures concerning the withdrawal, substitution and discharge of collateral are in place and adhered to.

2.6 Credit Disbursement

2.6.1 A pre-disbursement checklist is necessary to ensure that all security and legal documentation are in order and complete and conditions precedent are fulfilled before the disbursement of credit. It is the responsibility of the loan administration officers to ensure that all pre-disbursement conditions are complied with by the borrowers before the release of credit facilities is approved by the appropriate authority.

2.6.2 The internal auditor's scope of coverage should include the following:-

(a) Pre-disbursement checklist is duly signed off by the loan administration officer and approved by the relevant authority before the loans proceeds are released to the borrowers;

(b) Loan proceeds are released in accordance with the approved terms and conditions.

2.7 Credit Monitoring, Supervision and Recovery

2.7.1 Loan accounts should be reviewed prior to renewal, enhancement, reduction or restructure of existing credit exposures. This review normally includes analyzing the borrower's periodic financial statements and financing requirements, reassessing collateral values, making site visit to the borrower's business premises and keeping abreast with trends and developments in the industry. An effective credit monitoring system could serve as an early warning system for detecting potential problematic loans. And the management can take prompt action or measures to safeguard the banking institution's interests. To ensure the banking institution's credit standards are met there should conduct proper credit supervision. An effective credit recovery system is essential to minimise loan losses should the loans turn non-performing.

2.7.2 In evaluating the banking institution's credit monitoring, supervision and recovery system, the internal auditors should determine whether:-

(a) Collateral is valued periodically to ensure that the credit exposures are within the margin of advance;
(b) Potential delinquent loans are identified in a timely manner and prompt follow-up measures are adopted;
(c) Inform the management about the status of the delinquent loans;
(d) Adequate review of all the loan accounts is conducted before the borrowers' existing credit facilities are renewed, enhanced, reduced and restructured;
(e) Borrowers are appropriately graded in relation to the risks; and
(f) Restructured/rehabilitated loan accounts are properly approved and closely monitored.

2.8 Accounting and Financial Reporting

2.8.1 Management has the responsibility to establish a proper accounting and financial reporting system. The accounting records should not only capture all the credit facilities granted but also proper classification of credit facilities by loan types and economic sectors. An effective financial reporting provide the management with information needed for credit management decision making and target setting.

2.8.2 The internal auditors should address the following areas:-

(a) Loans are properly accounted for, correctly stated, classified and disclosed;

(b) Reports on credit information that is to be submitted to the management and the board should be relevant, accurate, adequate and timely. This includes analysis of the loan profile, loan growth, income contribution and concentration of credit in relation to economic sectors and borrowers;

(c) Balances of the subsidiary loan records must match with the amount stated in the general ledger. Reconciliation should be made on timely basis and immediate action should be taken to resolve any differences. The reconciliation should be reviewed and approved by appropriate supervisory personnel;

(d) Pertinent loan information such as bumiputera / non-bumiputera, resident controlled status, director interested and economic sectors must be promptly recorded and independently verified to ensure accuracy;

(e) To ensure that the credit exposures reported in the management accounts and Bank Negara Malaysia statistical returns are correctly stated there must be adequate system in place; and

(f) Accounting policies on income recognition, provision for losses and suspension of interest on non-performing loans are consistently applied.

2.9 Accounting and Financial Reporting

2.9.1 The management is responsible for ensuring that the credit facilities granted to borrowers do not breach any provisions of the BAFIA, Islamic Banking Act, Insurance Act, Takaful Act, directives and guidelines issued by Bank Negara Malaysia from time to time and others law and regulations. In addition, the credit operations should adhere to the rules issued by the banking associations.

2.9.2 The internal auditors should review the banking institution's compliance with legal and regulatory requirements, in particular, the following:

(a) Loans and advances are not granted against the security of the banking institution's own shares;

(b) Unsecured credits are extended in excess in compliance with the provisions of the BAFIA;

(c) Credits are not extended in excess of single customer limit imposed by Bank Negara Malaysia;

(d) No extension of credits to directors, staff and their interested concerns other than those permitted;

(e) No approval of credit facilities in excess of the credit officers' delegated limits; and

(f) No extensions of loans beyond the threshold limit imposed by Bank Negara Malaysia from time to time (for example, loans secured against shares and unit in unit trust).

2.9.3 The internal auditors should determine that there is adequate system in place to ensure the following:-

(a) Classification and suspension of interest on non-performing loans and provisioning for bad and doubtful debts comply with the minimum requirement of BNM/GP3 (Guidelines on the Suspension of Interest on Non-Performing Loans and Provision for Bad and Doubtful Debts);

(b) Credit facilities are classified correctly for the computation of risk-weighted capital adequacy ratio;

(c) All large exposures to Bank Negara Malaysia are promptly and accurately reported;

(d) CLASS data are accurate and reliable before they are submitted in diskette media to Bank Negara Malaysia in conjunction with the third quarter review of the adequacy of provision for bad and doubtful debts;

(e) Loans to priority sectors and non-residents are correctly classified and reported; and

(f) Statistical information submitted to Bank Negara Malaysia in relation to credit is correctly reported.

3. TREASURY OPERATIONS

3.1 Introduction

The function of the treasury department in a banking institution is to carry out foreign exchange (FX) and money market transaction (MM). FX transaction carried out for trading and for covering commercial deals arising from internal trade, money transfer and foreign investment. Meanwhile, MM operations cover both borrowing and lending activities and the trading of financial instruments. The management needs to further strengthen the related operating control as there are high exposures and risks associated with FX operations.

3.2 Risk Inherent in Treasury Operations

The major risks associated with treasury operations are exchange rate, credit, interest rate, country and operational risks. Management should establish an effective system of internal control to identify, control and manage these risks. An effective system of internal control should encompass a well defined organisational structure, clear formulation of policies and procedures, reporting requirement and accounting guidelines. Internal auditors should evaluate that the system of internal control designed is capable of identifying, monitoring and managing the major risks associated with treasury operations.

3.3 Policies and Procedures

3.3.1 The banking institutions should establish clear and comprehensive policies and operating procedures for treasury operations. Board should approve the policies and procedures. The policies and procedures should be periodically reviewed and updated to reflect changes in market practices, economic conditions and regulations. The policies include the trading objectives and strategies, management control and supervision of FX and MM trading activities, duties and responsibilities of dealers, approving authorities and discretionary limits, approved list of brokers, operational and counterparties limits and trading hours outside normal business and off-premises dealings. The operating procedures should cover settlements, extension and cancellation of contracts, giving of preferential rates, approval and duration for excesses, and detailed descriptions of accounting, revaluations and reconciliation processes.

3.3.2 The internal auditors should address the following areas of audit concern:

a. Adequacy of and compliance with established policies and procedures;

b. Treasury operations are in line with the objectives and strategies of the asset and liability management and the approved policies and procedures;

c. Proper segregation of duties and responsibilities relating to dealing, processing, settlement, accounting, revaluation and reconciliation function are practised;

d. Adequacy of and compliance with internally approved trading limit;

e. Amendments made to contracts are properly authenticated;

f. Inward and outward confirmations are verified and matched. Any discrepancies are checked immediately with the counterparties and recorded in the log book, and any unusual or irregular transactions are investigated;

g. Dealing positions of foreign branches and other related offices are adequately monitored;

h. Independent revaluation of foreign currency accounts is performed on periodic basis;

i. Settlements of FX and MM transactions are in accordance with the instructions stipulated in the contracts; and

j. Proper controls exist over the transfer of funds either through SPEEDS or SWIFT and transfer of ownership of debt securities issued through scripless securities trading systems.

3.3.3 Internal auditors should be alert of transactions which are exceptional or highly speculative in nature. When such transactions are suspected, the scope of coverage should be extended.

3.4 Asset and Liabilities Management (ALM)

3.4.1 Functionally, ALM plays the role of interest rate management, liquidity management and assets and liabilities maturity matching. Therefore, ALM deals with the strategic issues such as the structure of the balance sheet, proportion of capital to total assets, quality of earnings and maintenance of liquidity requirements.

3.4.2 The internal auditors should review the system used by ALM in managing the risks associated with FX and MM transactions.

Internal auditors should review the past performance to assess the profitability and liquidity of the banking institution's asset and liability structure in response to the interest rates sensitivity, interest re-pricing and maturity gaps of its assets and liabilities. Internal auditors should also be concerned with the relevancy, accuracy, reliability and timeliness of information generated for management's attention and decision-making.

3.5 Accounting and Financial Reporting

3.5.1 The internal auditors should determine whether:-

a. Recording, revaluation and income recognition of FX and MM transactions are carried out promptly and in accordance with Approved Accounting Standards;

b. Adequate accounting records in preparing the positions reports and for revaluation of FX positions; and

c. The reconciliation of all nostro account is frequently performed and all unreconciled items are timely resolved;

3.5.2 The assessment of the reliability of the system used to generate the management reports and Bank Negara Malaysia statistical returns should be done by the internal auditors. The reporting and types of reporting should be addressed in the policies.

3.6 Legal and Regulatory Requirements

3.6.1 The internal auditors should review the compliance with legal and regulatory requirements, particularly, with regard to the following:

a. Properly accounted for repo transactions;

b. Net open position of FX is within the limit set by Bank Negara Malaysia at all times;

c. Proper classification of FX transactions into trade and non- trade;

d. Accurate reporting of FX transactions for the purpose of capital adequacy requirement; and

e. Code of ethics and code of conduct issued by The Forex Association of Malaysia and Bank Negara Malaysia respectively are complied with.

4. DERIVATIVES

4.1 Introduction

4.1.1 The Guidelines on Minimum Standards on Risk Management Practices for Derivatives issued by Bank Negara Malaysia is about the banking institutions operations. The internal audit coverage under this section should be read in conjunction with the above guidelines.

4.1.2 To carry out their audit effectively, the internal auditors must be conversant and knowledgeable about derivative products and transactions, and must be guided by comprehensive audit manuals and programmes. Besides that, they must also be familiar with all relevant regulations and guidelines governing derivatives activities in order to evaluate the banking institution’s compliance.

4.2 Risk Inherent in Derivatives

4.2.1 Risk inherent in the derivatives include market, credit, operational, liquidity and legal risks. The internal auditors should assess whether risk exposures assumed by the banking institutions either have become too excessive vis-à-vis its capital position or have not been timely identified to the extent that they represent an unsafe and unsound banking practice.

4.2.2 The internal auditors should review whether the banking institutions have complied with the requirement on common integration of risks, risks measurement, limits and reporting, and management evaluation and supervision. Periodic review on the risk management models used by the banking institutions should be conducted by the internal auditors.

4.2.3 The internal auditors should determine whether the management and officers involved in derivative operations are fully aware of the risks associated with all on and off-balance sheet transactions and whether such transactions are carried out for hedging or speculative purposes. In addition, they should also ascertain whether exercised caution when the banking institutions are involved in over-the-counter derivative transactions. The nature and types of derivatives products, why and how they are transacted would dictate the level and amount of risk that the banking institutions are prepared to assume.

4.3 Policies and Procedures

4.3.1 The banking institutions should have written policies and procedures on derivatives operations that include parameters on risk activities, types of derivatives product traded, approving authorities and discretionary limits, review of various operational and counterparty limits and list of traders. It should also cover: organisational structure and job responsibility; reporting requirement; monitoring and stop loss mechanism; permissible activities; approved list of brokers and counterparties ;dealing guidelines (including off-market transactions and off-premises dealings); pricing assumptions, model and mechanism; dispute resolution methodology; detailed descriptions of transaction processes; settlements, accounting, revaluation and reconciliation procedures.

4.3.2 The internal auditors should review the banking institution's compliance with the following significant areas:-

a. All significant policies regarding to the management of derivatives risks should be approved by the board. These policies should be in line with the organisation's approved broader business strategies, capital strength, management expertise and overall willingness to take risks;

(b) In carrying out the approved policies the management should ensure that there are adequate operational guidelines and procedures in place for conducting derivatives operations on both long-range and day-to-day basis. This responsibility is to ensure that there are:-

(i) Clear delineation of lines of responsibility for managing risks;
(ii) Effective system for measuring risk;
(iii) Comprehensive risk- reporting process;
(iv) Appropriate limits on risk takings;
(v) Adequate dealing, processing and settlements procedures and effective system of internal control;
(vi) Effective monitoring and enforcement at all levels of management;
(vii) Sufficient resources and competence to carry out daily operations and risk management functions effectively;
(viii)Adequate revaluation procedures for derivatives transactions; and
(ix)Adequate pricing models or mechanism for derivatives.

(c) A committee has been set up to approve, oversee and control the derivative activities;

(d) To ensure the derivatives activities are conducted according to the establish policies and guideline and to do the research and make recommendation pertaining to the risk measurement methods and control policies an independent research unit are set up;

(e) The development of risk policies and the process of measuring, monitoring and controlling risk should be performed independently by an individual that conducts the derivatives activities (marketing, dealing, processing). The individuals or unit responsibility for these functions must be able to report risk exposures and compliance with control procedures independently to both the management and the board;

(f) New derivatives activities should be avoided until the management has acknowledged and fully understood the activity and is in a position to oversee or manage the new activity; and

(g) Derivatives are offered to customers as for the hedging purposes and the assessment on the suitability of the derivatives products offered is adequate.

4.4 Accounting and Financial Reporting

4.4.1 To ensure that there is a prudent operation of derivatives activities, it is essential to ascertain there are an accurate, informative and timely accounting, management and financial reporting system. The quality of MIS is an important factor in the overall effectiveness of the risk management process. All the reports pertaining to the derivatives operations submitted to the management and the board should be in line with the requirements of the BNM guidelines.

4.4.2 The internal auditors should ascertain whether the accounting and reports preparations are being carried out by persons or units independent of dealing and marketing function. The audit scope should at least cover the following :-

(a) Written accounting policies relating to trading and hedging with derivatives instruments conform with Approved Accounting Standards;

(b) The accounting records should accurately state the cost and market value of derivatives transactions;

(c) Hedging transactions meet the criteria for exclusion from classification as trading transactions;

(d) Appropriate method is used to measure to value the derivatives positions and that assumptions underlying those methods are reasonable;

(e) Revaluations procedures address the full range of trading instruments;

(f) Market rates used for evaluation are independently obtained;

(g) All off-market transactions and off-premise dealings are properly accounted for and reported; and

(h) Level of profit and risk positions are assessed based on earnings and risk reward profile of specific products.

4.5 Legal and Regulatory Requirement

The internal auditors should review whether the relevant laws, regulations and guidelines particularly the Minimum Standards on Risk Management Practices for Derivatives Issued by BNM have been complied with. Besides that, the internal auditors should also review the compliance with the rules issued by Securities Commissions, Kuala Lumpur Options and Financial Futures Exchange (KLOFFE) and Malaysia Monetary Exchange (MME).

5. INVESTMENT IN DEBT AND EQUITY SECURITIES

5.1 Introduction

Normally, financial Institution's in debt and equity securities involve participation in two main financial markets that is capital market and money and foreign exchange market. A typical investment portfolio consists of public debt securities, equity securities (quoted and unquoted), equity-link securities, Islamic and private debt securities. Equity securities and public debt securities may also be acquired in the primary market or as a result of underwriting commitment. In banking institutions, equity securities are also acquired in satisfaction of debt through debt-equity conversion. Investment and trading securities may account for sizeable proportion of the financial institution's asset and therefore, securities of inferior quality may have an adverse impact on the financial institution's condition.

5.2 Investment Strategy

5.2.1 An investment strategy should be established and approved by the board and regularly reviewed to take into account the changing market and economic condition. The strategy should include the investment objectives and goals, the size of the investment portfolio, the types and composition of the securities, quality and maturity structure and target yields for the overall portfolio. The investment strategy should also distinguish securities that are held for investment and trading purposes. A guiding principles in the investment strategy is to achieve profitable returns while at the same time, managing risks within the investment portfolio. The investment strategy adopted should commensurate with the risks that the financial institution is prepared to assume.

5.2.2 For the purpose of analyzing various investment activities the formulation of policies and procedures should be made by the management. This is to meet the organisation's objectives after taking into consideration the level of management expertise, the sophistication of the financial institution's control procedures and monitoring systems, its asset and liability structure and its capacity to maintain liquidity.

5.3 Risk Inherent in Investment

The risk inherent in investment includes credit, price, liquidity, operational and country risks. The level of the risk inherent in investment depends on whether the investment is held on long term or short term and the complexity of the investment products. The internal auditors should review the mechanism used by the management ti identify and manage these risks.

5.4 Policies and Procedures

5.4.1Management should establish comprehensive policies and procedures for investment operations. These policies should be approved by the board and subject to periodic review to conform with the asset liability management's (ALM) strategy. Investment stratyegy should take into account the objectives and goals, exposure limits for each major type of investment, basis for assessing risks of alternatives investments, approving authority and discretionary limits for the purchase or disposal of investment, evaluation and selection of securities dealers and custodians, revaluation of investment and recognition of income and losses. The policies should also cover the basis of classification of investment either for investment or dealing purposes. Establish procedures should include organisational structure of investment officers, monitoring mechanism and reporting requirement.

5.4.2 The internal auditors should focus on the following significant areas:-

(a) Adequacy of and compliance with policies and procedures;

(b) Investment operations are in line with the investment strategy;

(c) Segregation of duties for trading, processing, custody, payment and receipt, and maintenance of subsidiary records and accounting functions is practised;

(d) No over concentration of investment in a particular counter, sector or types;

(e) Trading and exposures limits imposed by the board are not breached;

(f) Payment is only made upon receipt of the confirmation of transfer of security, particular in the case of scripless negotiable instruments of deposits or instruments that are normally entrusted with a central depository or an authorised depository;

(g) Share certificates or shares that are prescribed under the Central Depository System are registered in the name of nominee company;

(h) Revaluation exercise is carried out on the investment portfolio at least on a monthly basis;

(i) Adequate provision for permanent diminution in value has been made for securities of inferior quality; and

(j) Securities borrowed or lent out are properly accounted for.

5.5 Accounting and Financial Reporting

5.5.1 The accounting and financial reporting of investment in debt and security should conform with Approved Accounting Standards. The classification of debt or equity securities must accord with the approved policies, as either for investment or dealing purposes. Such classification should be determined at the outset of the acquisition, and any subsequent reclassification should be approved and properly documented.

5.5.2 The internal auditors should evaluate the relevancy, accuracy, frequency and timeliness of reports submitted to the management and the board. Such report should cover all types of investment, gains or losses from disposal, provision for diminution in value and transfer of securities between investment and dealing securities.

5.6 Legal and Regulatory Requirement

5.6.1 The financial institutions' investment should comply with the regulatory requirements issued by BNM and various regulatory bodies from time to time. The internal auditors should verify that the investment is within the limits for investment in private debt securities and for investment in shares.

5.6.2 In some financial institutions where investment operations unit handles both the financial institution's own investments and the clients' investment portfolio, internal auditors should determine whether the financial institutions have observed the spirit of BNM/GP7 (Guidelines for the Code of Conduct for Directors, Officers and Employees in the Banking Industry) on the code of ethics in the acquisition of the investment instruments.

6. INFORMATION SYSTEMS

6.1 Introduction

6.1.1 For the purpose of these guidelines, information system (IS) refers to an environment where a computer of any type or size is used to process information that is significance to the audit. In an IS environment, the overall audit objectives and scope do not change. However, the use of a computer changes the processing and storage of information, and the traditional visible audit trails may no longer exist. Accordingly, the audit procedures in the evaluation of the computerised system and internal control would be different from those used in the review of a manual system. The review of an IS processing function would required specialized knowledge and skills due to the loss of visible audit trail. In order, to evaluate the internal controls of the computerised system the financial institution should have an effective IS audit function.

6.1.2 In this section, it describes the minimum coverage in performing an IS audit. Particularly, the IS auditors should review the effectiveness of IS in supporting the business activities of the financial institution and the adequacy of control over the IS management, systems development and programming, computer operations and security, teleprocessing and data integrity. And this section also includes the minimum IS audit coverage for the electronic coverage for the electronic funds transfer (EFT) systems and credit card operations.

6.2 Management

6.2.1 The management have the primary responsibility for the overall system of internal control. Financial institution should establish an IS security policy, in line with the emerge of more complex systems and the need to protect financial institution's resources and customers information. This policy should provide guidelines on the administration of security to ensure the confidentiality, integrity an availability of the computerised system.

6.2.2 In reviewing the IS management function, the IS auditors should pay particular attention to the following: -

(a) IS strategic plan is in place;

(b) IS strategic plan is consistent with the financial institution's business objectives and goals;

(c) Participation from the internal audit department is included if an IS steering committee is established;

(d) Standard and procedures on the various IS activities such as systems development and programming, computer operations and security, teleprocessing and computerised applications are adequate and in compliance with the IS security policy;

(e) The organizational structure of the IS department provides proper reporting line. Segregation of incompatible functions within the IS processing activities is practiced (i.e systems development and programming, computer operations and security implementation). The IS auditors should determine the adequacy of compensating controls where in cases such segregation may not be possible and normally found in small IS installations;

(f) Management reports on the IS activities are adequate and effective in monitoring IS performance and in assisting management to make business decisions;

(g) IS staff and users are adequately trained; and

(h) IS activities have complied with relevant guidelines issued by BNM from time to time.

6.3 System Development and Programming

6.3.1 Failure to use proven system development and implementation methodology could result in significant financial losses. Therefore, to ensure the reliability and integrity of computerized system installed, it is imperative that management provides adequate controls over the entire process of acquiring/ developing computerized systems. Systems development and programming standards established by the management should provide general guidelines on the design, programming, testing, conversion, implementation, documentation, maintenance of application and operating systems, software and hardware selection and acquisition, and post-implementation review.

6.3.2 The IS auditors' role in the systems development and programming function should not only be limited to the auditing of system already implemented. To ensure that appropriate that appropriate audit and control procedures are design and built into the systems the IS auditors should also participate, in consultative/ advisory capacity, in the development of new computerized systems. While participating in the systems development process, the IS auditors should maintain objectivity and independence from any operational responsibility of the system being developed. In the review of the systems development and programming functions, the IS auditors' main areas of concern include the following:-

(a) Standards and procedures on the systems development and programming function are available and comprehensive;

(b) The development of application has complied with the standard on the systems development and programming function;

(c) An effective project management system is employed to monitor and control application development projects;

(d) Application programmers do not have "write" access to production data and are not involve in the maintenance of operating systems software. Similarly, system programmers should not have access to production data and are not involve in the maintenance of application programmers

(e) Production system is properly segregated from the development or testing systems;

(f) Documentation maintained on the application systems is comprehensive and current. The documentation should at least include user manual, computer operator instructions, flowchart and the description of the application systems and programmes.

(g) To ensure the integrity of data and programmes in the systems, therefore, controls over the maintenance of application programmes and operating systems are adequate and effective.

Procedures should ensure that all requests for changes are authorized and attended to timely. Only authorized programmes are catalogued to the production system and the relevant documentation updated to reflect the changes. Controls over urgent request for application programmes or operating system changes should also be in place since such request would normally bypass the need for prior return authorization;

(h) Test plan and test result are adequately maintained for review;

(i) Controls over the usage of powerful utilities with data altering capabilities are adequate and effective; and

(j) Procedures to review purchase agreement and service contract for hardware and software are available and adequate to protect the financial institution's interest before they are executed.

6.4 Computer Operations

6.4.1 It is under the responsibility of the computer operations to ascertain the efficiency and timely processing of data and the maintenance of the computer system. In general, the computer operation should cover operations and the maintenance of the computer equipment and its peripheral, problem handling and housekeeping of the computer room. With regard to the system reliability and availability, management has the responsibility to formulate the comprehensive disaster recovery plan, including identification of alternative processing site and alternative processing capability.

6.4.2 The IS auditors should pay particular attention to the following areas:-

(a) Computer operations are adequate and complied with;

(b) Physical controls over the computer are adequate and effective. The controls may consist of access restriction to the console, teleprocessing equipment and back-up media library, maintenance of the computer room and installation of adequate protection against fire, flood and disasters;

(c) Adequate controls to ensure correct tapes, disks or other storage media are used and data files are correctly written or read;

(d) Adequate detective and preventive controls are in place; and

(e) Procedures for the disaster recovery plan comply with BNM guidelines.

6.5 Computer Security

6.5.1 To ensure that unauthorised changes cannot be made to production programmes, operating systems and data the management is responsible to institute adequate controls. Procedures should also be formulated by management on the implementation of the security administration function.

6.5.2 In assessing the adequacy of computer security, the IS main areas of concern should include the following:-

(a) The security administration function is clearly and properly assigned to a competent staff;

(b) Adequate and effective procedures on security administration that include password issuance and maintenance, and follow-up on access violations;

(c) Assignment of access capabilities to users is properly done and in accordance with the access rule. Access to sensitive resources such as procedures libraries, powerful data and program altering utilities, system parameters, log and password file should be restricted. If a database management system are used, the assignment of access to database should also be reviewed to ensure proper assignment of capabilities;

(d) Logging, reporting and reviewing of activities, especially abnormal activities are adequate and effective; and

(e) Security policies is communicating to the users.

6.6 Teleprocessing

6.6.1 The diversification of information delivery channel poses an increased risk to data security through unauthorized access to a system. Management should ensure that adequate controls have been constituted over the financial institution's teleprocessing network to determine data transmitted are complete, accurate and authorized, routed to the correct destination and transmission errors are detected and corrected.

6.6.2 The auditors should look into the following areas in reviewing the teleprocessing system :-

(a) Procedures on teleprocessing are adequate and complied with. The procedures should at least include measures to restrict access to files, transactions and terminals, logging, reporting and reviewing deviations from normal transactions and backup procedures;

(b) The security implemented such as encryption, call back and error detection techniques were to protect transmitted data over the telecommunication media is adequate;

(c) All transmissions are received from authorized terminals and users;

(d) Procedures on error detection and recovery are adequate and effective;

(e) Network activities are logged, reported and reviewed by the network supervisor; and

(f) Procedures are adequate to ensure system reliability.

6.7 Data Integrity

6.7.1 To process their operational activities, most financial institutions have installed computerized application systems and this system is either develop in house or purchase from external vendors. Therefore, the accuracy and integrity of data are dependent upon the establishment of proper control procedures (programmed or manual) for transaction processing in both the user and IS departments of the financial institutions.

6.7.2 The IS auditors should conduct specific application review to test the integrity and reliability of data in specific application system. In such review, the IS auditor should strive to use Computer-Assisted Audit Techniques (CAATs) since this approach could improve the checking of data integrity auditing “through” the system rather than relying only on the validation controls of input and output, The areas of concern in conducting such review are as follows: -

(a) To ensure accuracy and completeness of data and to prevent initiation of transactions by unauthorized personnel, it is important to ascertain that the controls over the input of data are adequate and effective;

(b) Programmed controls for example edit checks, reasonable checks are adequate to ensure processing of information are correctly done. Such controls should include procedures on handling rejected and resubmission of data; and

(c) Controls over output distribution are adequate. A comprehensive set of exception and discrepancy reports should be provided to authorized personnel for verification and error correction purposes.

6.8 Electronic Fund Transfer (EFT) System

6.8.1 Two types of EFT system that is installed in the banking institutions are wholesale EFT system which include SPEEDS and SWIFT, and retail EFT system that consist of Automated Teller Machine (ATM), Point-of-Sale (POS) system and debit cards. It is under the management responsibility to establish policies and procedures for the EFT system which provide guidelines on the approving authority and discretionary powers, organization of records and files, internal supervision in identifying irregularities and the relevant follow-up or punitive actions to be taken

6.8.2 In reviewing the wholesale EFT system, the IS auditors should pay particular attention to the following:-

(a) Internal policies and procedures on funds transfer activities are adequate and complied with;

(b)Controls over origination of input documents, processing and output are adequate;

(c)Teleprocessings are adequate to ensure the confidentiality, integrity and availability of data transmitted over the system;

(d) Enforcement on the segregation of function is done. For example, security administration, data entry and transmit functions should be segregated. Where data entry and transmit functions are not segregated for certain discretionary limits, adequate compensating controls should be in place;

(e) Sensitive items, such as master password and log-in tables are kept under dual custody;

(f) To minimize the exposure of erroneous transfer of funds or to detect unauthorized transfer of funds the reconciliation of the number of messages and value of the funds transmitted is performed on timely basis;

(g) Reports are printed to monitor the activities in the SPEEDS/SWIFT system are adequate; and

(h) Physical security over the SPEEDS/SWIFTS terminals, records, equipment, source documents and systems-generated report is adequate.

6.8.3 In reviewing the retail EFT system, the IS auditors should pay particular attention to the following:-

(a) Procedures on the ATM operations are available and adequate;

(b) Controls over the procurement, processing, storage and distribution of plastic cards and PIN mailers are adequate;

(c) PINs are encrypted on all files and databases during transmission;

(d) Sensitive items, such as PIN keys used during PIN generation and verification, and documentation on the encryption, decryption and PIN generation process are securely kept;

(e) Segregation of incompatible functions is practiced. Card processing and custodianship should be segregated from PIN processing and custodianship;

(f) User-ids and passwords to access the systems have been assigned to authorized personnel:

(g) Controls over originations of input documents, processing and output distribution are adequate;

(h) Procedures on the PIN generation process are adequate including the deletion of any recording medium used in the process of assigning, distributing, calculating or encrypting PINs immediately after used;

(i) The financial institution has complied with applicable laws and guidelines issued by BNM; and

(j) For shared ATM network;

(i) Adequate audit trails are maintained for all transactions;

(ii) Rejected items are properly reported and accounted for; and

(iii) Procedures on balancing and setting transactions are adequate.

6.9 Credit Card Operations

6.9.1 Credit card facility is a form of payment and banking arrangement introduced to facilitate the purchase of goods and services by consumers. One of the risk inherent in the credit card operations is credit risk. This credit risk elaborated in the Credit Operations of Part V of these guidelines. It is the responsibility of the management to establish policies and procedures which should provide guidelines on approving limits, credit appraisal and supervision, card processing and custodianship, merchant recruitment and termination, MIS and record keeping for this facility.

6.9.2 The IS auditors' minimum audit coverage in the review of the credit card operations is as follows:-

(a) Policies and procedures governing the credit card operations are adequate and complied with;

(b) Incompatible functions within the credit card operations are segregated. For instance, the card processing function such as card approval, transaction authorization, accounting, card embossing and card distribution should be segregated;

(c) No credit limits in excess of the approving officers' authority are given to approve credit card applications;

(d) Procedures of input, processing and output of credit card applications and transactions are adequate to ensure accuracy, completeness and validity of data entered into credit cards application systems;

(e) Procedures on the assignment and maintenance of user-ids and passwords to the credit card application system are adequate and effective;

(f) Controls over the maintenance of account status such as deactivation of card reported lost/stolen are adequate;

(g) Controls over the procurement, embossing and encoding, storage and distribution of credit cards are adequate;

(h) Procedures on the PIN generation process are adequate. These include the deletion of any recording medium used in the process of assigning, distributing, calculating or encrypting PINs immediately after use (ATM systems);

(i) Management information systems are adequate. This includes reporting of, at least, accounts in excess of limits, accounts with arrears, non-performing loans, accounts with disputes, daily excess authorization report and fraud cases; and

(j) Generally, the financial institution has complied with applicable laws and guidelines issued by BNM.

7. INSURANCE UNDERWRITING

7.1 Introduction

The principal activity of an insurance company is underwriting of risks. Insurance underwriting deals with the principles and practices concerning the acceptance or rejection of risks, fixing of premium rates, terms and conditions, the amount of acceptance, retention and reinsurance. This section describes the minimum audit coverage which internal auditors must perform when reviewing the underwriting process of the insurance company.

7.2 Risks Inherent in Underwriting

7.2.1 Risks associated with the underwriting process include timing, investment return, credit, expenses and loss occurrence risks. When developing the underwriting strategy for the company the management should address all the risks.

7.2.2 The internal auditors should review the mechanism used by the management to identify and manage the risks associated with underwriting.

7.3 Policies and Procedures

7.3.1 Management has the responsibility of managing the risks prudently. Hence, it is essential for the management to have in place sound underwriting policies, procedures and a well established system of internal control.

7.3.2The underwriting policies which are formalized and approved by the board should at least cover the setting of authorized limits for officers and intermediaries, retention limits for each class of business or types of life products, guidelines on appointment of agents, controls on the acceptance of business, conditions for requiring pre-acceptance survey/medical check-up, portfolio mix requirement (general Insurance), ratings and terms.

7.3.3 The internal auditors should address the following areas of audit concern:-

(a) Adequacy of policies and procedures;

(b) Compliance with the company's underwriting policies and procedures and adequacy of the internal controls governing the underwriting process;

(c) Accumulation of risks (general)/ multiple policies (life) are checked by underwriters prior to acceptance of risks;

(d) Controls exists over the acceptance and change of risks and subsequent issuance of policy and endorsement documents. This would include controls instituted over proposal forms, checking of policy documentation and dispatch of policies to policyholders;

(e) Controls exist over the collection of premium monies from direct clients and intermediaries;

(f) Procedures governing the issuance of renewal notices are in place;

(g) Procedures are instituted over the appointment and conduct of intermediaries, in particular the monitoring of errant intermediaries. This would minimise the possibilities of intermediaries giving false representations on policy benefits, terms and exclusions; and

(h) Adequate controls are instituted over the safeguarding and issuance of cover noted to general insurance. These controls are critical as the insurers are at risk upon the issuance of cover notes by the agents. The cover note control system for motor business should include matching of Road Transport Department (RTD) copies of cover notes to the records of companies.

7.4 Reinsurance

7.4.1 Reinsurance is an arrangement whereby an original insurer transfer a part of the risk to another insurer or reinsurer. The method for arranging reinsurance can be through facultative or treaty basis.

7.4.2 Fixing of retention is the primary factor in the placement of reinsurance (i.e. risk above retention would have to be reinsured)

7.4.3 The internal auditors should ascertain the following for reinsurance: -

(a) All risk over specified retention limits are reinsured with treaty reinsurers which are good security and approved by the company. The company should have an established system for vetting the quality of reinsurers, reviewing their financial standing and setting limits of exposures to any one reinsurer;

(b) Risk ceded is in accordance with the terms of the reinsurance contract and premiums ceded on reinsurance arrangement are properly recorded and reported to reinsurer;

(c) Facultative reinsurance arrangements are made prior to the acceptance of risks for risks which have exceeded treaty limits;

(d) The company ceded to Malaysia National Reinsurance Berhad (MNRB) in accordance with the voluntary cession agreement;

(e) Reinsurance arrangement provides adequate protection for all classes of business accepted and that facultative reinsurance (where applicable) has been properly placed and leaving no gap in cover;

(f) Utilisation of the Excess of Loss (XOL) treaty is monitored and the reinstatement premium is computed;

(g) For reinsurance placement made through brokers, the brokers should be reputable standing and are required to promptly submit placement slips, signed reinsurance policies or treaty documents to the company;

(h) Reinsurance programme is reviewed annually to ensure that reinsurance needs are properly and adequately met; and

(i) Reinsurer statement of accounts are regularly reconciled and reconciling items are timely followed up.

7.5 Accounting and Financial Reporting

7.5.1 It is the management responsibility to establish a proper and effective accounting and financial reporting systems. The company's accounting records should captured all the financial transactions of the company. An effective financial reporting systems provides the management with the necessary information needed to manage the underwriting portfolio and to make business decisions.

7.5.2 The internal auditors should pay particular attention to the following:-

(a) Reporting systems provides accurate statistical records of the company's underwriting data to enable management to make appropriate analysis and to project the direction of the company;

(b) The premium recording system for life business is adequate and reliable in generating the appropriate analysis of information for use in the calculation of long term liabilities (actuarial valuation) and updating the master life;

(c) Reports to management and the board are relevant, accurate, adequate and timely;

(d) Premiums, reinsurance premium ceded, return premiums and commission expenses are correctly stated and properly accounted for in the company's records. Revenue for life business is only recognized to the extent that it is due with respect to policies in force and as for the general business the revenue is recognized when the premiums are received;

(e) Commissions payable and receivable are accurately and completely accounted for; and

(f) Adequate provision is made for amounts due which have been outstanding for more than six months.

7.6 Legal and Regulatory Requirement

7.6.1 It is under the responsibility of the management to ensure the compliance with all legal and regulatory requirement. The internal auditors should review compliance with the Insurance Act 1996, Takaful Act 1984 and other applicable laws, official circular, guidelines and derivatives issued by BNM, PIAM and LIAM.

7.6.2 The internal auditors should review the company compliance with legal and regulatory requirement, in particular, the following:-

(a) Premium rates for life business are charged in accordance with the rates approved by a qualified actuary meanwhile as for tariff rated class of general insurance business, the premium are charged in accordance with the tariff;

(b) Register of policy is maintained as prescribed by the Insurance Act 1996 and Takaful Act 1984;

(c) Only registered agents are allowed to transact insurance business on behalf of the company;

(d) Commission that inclusive of agency related expenses and other benefits are paid to the intermediaries in accordance with the limits stipulates in BNM’s Operating Cost Control Guidelines (OCC);

(e) Management expenses of the company do not exceed the limits stipulated in the OCC;

(f) Payments and remittance of motor premiums comply with insurance regulations;

(g) Payment of premium to the insurance companies within 60 days of commencement of risk that is for most classes of general insurance is in compliance with premium warranty clause; and

(h) Local retention is optimized and fronting arrangements with foreign insurers are avoided.

7.6.3 The internal auditor should determine whether management review and supervision are in place to ensure accuracy of the data or information reported in the returns submitted to BNM

8. INSURANCE CLAIMS

8.1 Introduction

8.1.1 The integral part in the insurance business is the claims arising from the insurance policies. In order to identify types and extent of losses, the provision required, accounting and financial requirement the insurance should have a system in place. The claims process includes the recording of initial intimation of loss, verification of details, determination of the extent of the liabilities, estimation of the amount to be settled, settlement of claims and recoveries of reinsurance. As for the insurance companies that carry out general business the claims process would include recoveries for knock for knock agreements, salvage and subrogation

8.1.2 The largest liability item in the balance sheet of a general insurance company usually is the reserve for outstanding claims. Any material underprovision in the reserve for outstanding claims or the use of inaccurate method of determination would have a significant impact on the insurer’s financial position. The estimation for outstanding claims in general business is critical as it is an area of unconsiderable uncertainty and frequently involves the subjective judgments of insurers. However, the reserves for outstanding claims in life insurance business are easily determined based on the principal sum assured and the bonuses declared. Occurrence of claims in life policies is usually either upon death or maturity.

8.1.3 Past statistics on abuses in claims have indicated that such abuses are more prevalent in general business particularly motor business than in life business. Accordingly, this section deals more with the scope of audit coverage on general claims. However, in the course of audit of life claims, the internal auditors should adopt this section wherever applicable.

8.2 Policies and Procedures

8.2.1 It is under the responsibility of the management to establish proper and sound policies and procedures pertaining to administration of the claims portfolio. These policies and procedures may be in the form of manual or guidelines. The policies on claims that is approved by the boards covers approved limits for competent personnel and the claims committee, prompt and fair settlements of claims, reporting on large losses, payment on claims of claims on ex-gratia basis and appointment of loss adjusters, surveyors and solicitors. The claims procedures usually provide detailed guidelines on the various claims processes including sales or disposal of wrecks, basis of determining reserves for outstanding claims including incurred but not reported (IBNR) and processing and disbursement of claims.

8.2.2 The internal auditors should address the following areas of audit concern:-

(a) Adequacy of policies and procedures;

(b) Claims process complies with the approved policies and procedures;

(c) Segregation of duties and responsibilities relating to claims processing, approval and p[payment is practised;

(d) Register of claims is maintained as prescribed by the Insurance Act 1996 and Takaful Act 1984, All claims or known losses should be promptly registered with reasonable provision (even in cases where limited information is available)

(e) Claims data are accurately recorded;

(f) Proper and fair claims settlement practices have been adopted:-

(i) Prompt in processing and paying claims and no ‘delay tactics’

(ii) Disbursement of claims are properly approved and supported by appropriate documentation;

(iii) Preventive measure are in place to deter fraud; and

(iv) Requirement stipulated in guidelines issued by JPI on claims settlements practices and guidelines to combat motor insurance fraud (general business) are complied with.

(g) Estimates of preliminary loss reserves are reasonable, regularly reviewed and updated upon receipt of fresh and relevant information. Experienced and competent officers should review the reserves on every outstanding claim at least once a year;

(h) Claims settled through compromise or ex-gratia basis are reasonable, justifiable and not subject to abuse;

(i) All recoveries in respect of salvage, subrogation or from reinsurers are properly recorded and collected on a timely basis. In cases involving motor claims, adequate controls are instituted over the sale of wrecks;

(j) Outstanding loss of reserves inclusive of IBNR are adequate at any point of time. And for this purposes, IBNR established at the last balance sheet date would be regarded as IBNR required at any point of time until the next balance sheet date;

(k) Proper monitoring system is in place to record accumulation of claims arising from a particular events or within a particular period for purposes of reporting to XOL reinsurers and for review of adequacy of XOL cover; and

(l) A system is in place to identify maturing life policies to enable payments to be made promptly.

8.3 Incurred but not reported

8.3.1 The reserve for outstanding claims consist of two main components that is losses reported but not paid and losses incurred but not reported. Unlike the estimate for losses reported but not paid, the reserve estimate for IBNR is difficult to determine and may result in possible underestimation due to the unknown amounts of eventual losses. BNM has issued guidelines on IBNR claims provision with respect to direct and facultative accepted reinsurance business and this is to ensure that a prudent technical approach is applied to the estimation of IBNR claims.

8.3.2 The estimation of IBNR is not purely mathematical process as qualitative factors are also crucial inputs and would have bearing on the results of the estimation. It is therefore pertinent and critical for both the management and the internal auditors to have a good understanding of the insurer’s business portfolio, changes in underwriting, claims reserving, settlements practices, data processing and accounting practices as well as other factors which may have an impact on the insurer's liabilities.

8.3.3 In determining the reasonableness and adequacy of IBNR estimation, the internal auditors should:-

(a) Review and determine the insurer's compliance with the relevant guidelines especially on IBNR claims provision;

(b) Assess whether proper and adequate controls are implemented to ensure the integrity and completeness of data prior to conducting the mathematical estimation of IBNR;

(c) Review the reasonableness of all underlying assumptions used in methodology and estimation; and

(d) Obtain a reasonable and satisfactory explanation if the results of the mathematical estimation indicate the following estimation:-

(i) Estimated incurred claims ratios differ from the market average;
(ii) Mathematically derived results indicate reducing trend in claim ratios; and

(iii) Estimated outstanding claims are lower than the aggregate results of the case by case estimates.

8.4 Reinsurance Recoveries

8.4.1 The financial position of the reinsurers is paramount to the success of any reinsurance programme. The reinsurance programme will not benefit the reinsurer if the reinsurer does not have the financial capability in meeting all valid claims under the terms of various reinsurance agreements or settling those without undue delay.

8.4.2 In accessing the adequacy of loss reserves involving reinsurance, the internal auditors should determine that the company does not take credit or account for any reinsurance recoveries in cases where the reinsurer concerned has become insolvent, has rejected the claims, or claims recoveries have been outstanding for more than six months.

8.4.3 With respect to the facultative reinsurance arrangement, internal auditors should determine that the company keeps the reinsurers inform at all times regarding the developments of the claims. All major decisions made must be fully agreed upon by all facultative reinsurers particularly, in cases of disputed liability and quantum.

8.4.4 The internal auditors should also determine that the company credit the reinsurers for their share of claims recovered through subrogation or disposal value of salvage. The company should be prompt in recovering from the reinsurers upon payment of the claims.

8.5 Accounting and Financial Reporting

8.5.1 It is under the responsibility of the management to establish a proper accounting and financial reporting system. All the loss reserves intimated should be properly classified and captured in the accounting records.

8.5.2 The internal auditors should pay particular attention to the following:-

(a) Reporting systems provides accurate statistical records of the company's outstanding claims. This would provide management with the necessary information to analyse and project loss reserves in order to make provision for IBNR;

(b) Reports to the management are relevant, accurate, adequate and timely;

(c) Reserves for outstanding loss inclusive of IBNR are adequate and correctly recorded. Claims recoveries other than recoveries from reinsurance are only accounted for on receipt basis unless the realisation of the claims can be ascertains with reasonable certainty. The provision for claims should also include reasonable estimate of expenses arising directly from claims such as legal and adjusters fees;

(d) Payments of claims are accurately recorded and accordingly, provision for claims is reduced or eliminated immediately. For life business, such policies should be deleted from the master policy listing used in calculating actuarial reserves; and

(e) Balances of outstanding claims listing match with the balances in the general ledger. The reconciliation process should be functioning and any differences thoroughly investigated and resolved in a timely manner. The reconciliation should be reviewed and approved by the appropriate supervisory personnel.

8.6 Legal and Regulatory Requirement

8.6.1 The management is responsible for ensuring that the operations of the company in respect of the claims portfolio are in compliance with the applicable laws and regulations, guidelines and directives issued by BNM and other regulatory authorities and applicable rules set by various associations.

8.6.2 The internal auditors should review whether all applicable legal and regulatory requirement have been complied with. The internal auditors should also determine whether management review and supervision are in place to ensure that the figures reported in the returns submitted to BNM are accurate.

PART VL GLOSSARY

Administrative reporting –	Administrative reporting to CEO covers the application for leave, staff loans, advances and claims.
Auditable areas –	Any unit or activity within an organisation subject to audit
Auditee –	Any unit or activity within an organization that is audited.
Banking Institution (BI)-	For the purpose of the guidelines, BI refers to the collective reference of commercial banks, merchant banks and finance companies, which are licensed under Banking and Financial Institution Act 1989 or Islamic Banking Act 1983.
BNM/GP1 –	Guidelines on Directorship in Banking Institutions.
BNM/GP3 –	Guidelines on the Suspension of Interest on Non-Performing Loans and Provisions for Bad and Doubtful Debts.
BNM/GP5 –	Guidelines on the Credit Limit to a Single Customers.
BNM/GP7 –	Guidelines on Code of Conduct for Directors, Officers and Employees in the Banking Industry.
Chief Internal Auditors -	The person who heads the internal audit departments. Also called CIA.
Credit Facilities-	As defined under BAFIA, 1989 and Insurance Act 1996. For the purpose of the guidelines, credit facilities include hire purchase, leasing and block discounting, In the context of Islamic banking, credit facilities refer to financing and other facilities granted in accordance with the rules of shariah.
Financial Institution (FI)-	For the purpose of this guidelines, FI refers to collective reference to BIs, insurance companies and takaful companies licensed under the Insurance Act 1996 or Takaful Act 1984.
Hedging Transaction-	One that eliminates or limits the impact of interest or exchange rate movements on an existing asset or liability, or an identified future transaction.

Independent in Fact- The internal auditor's ability to take an unbiased viewpoint in the performance of his service.

Management – Person or group of people who provide the decision and the supervision to implement the financial institutions' objectives.

Management Audit – An activity which review management performance relating to an organisation's functions, systems, processes, operational controls and programs and projects. The audit would involve a performance appraisal of the activities of all levels of management. Also referred to as operational auditing, value for money auditing, performance auditing and efficiency auditing.

Over-The-Counter Transactions - Derivative transaction that are tailored to the counter-parties' requirements rather than being subject to the specification of any recognized exchanged.

Systems of Internal Control- The whole system of control, financial and otherwise, established by the management in order to carry on the business of an organization in an orderly and efficient manner, ensure adherence to management policies, safeguard assets and secure as far as possible the completeness and accuracy of records