

Chapter 8

Critical Areas of Operations: Risk Assessment and Management

Contents Outline

	Page
1. Introduction	2
2. Risks Faced by the Banking industry and Financial Institutions	3
3. Audit of Critical Operational Areas	6
4. Branch Operations	6
5. Credit Operations (Lending)	7
6. Treasury Operations (Money Market and Foreign Exchange)	18
7. Derivatives.....	24
8. Investments in Debts and Equity Securities.....	28
9. Information Technology	31
10. Other Operational Areas: Head Office Operations	40
11. Other Operational Areas: Insurance Underwriting And Claims	41
12. Other Operational Areas: Business Continuity Management	49
13. Other Operational Areas: Islamic Banking – The Shariah Committee.....	51
14. Other Operational Areas: Basel Capital Accord II.....	53
15. Outsourcing.....	54
16. Conclusion	55

Learning Objectives

After studying this chapter, you will:

- ◆ understand the rationale for the issuance and objectives of the BNM/GP10 Guidelines on Minimum Audit Standards for Internal Auditors of Financial Institutions for management of risks in financial institutions;
- ◆ appreciate the various types of risks in the business of banking;
- ◆ be familiar with the specific risks of each critical operation in a financial institution; and
- ◆ be able to apply the understanding of risks to the auditing of critical operations in a financial institution.

1. INTRODUCTION

The main objective of financial institutions is to maximise profits and enhance their shareholders' value. Financial institutions obtain funds (cash) from depositors in exchange for a promise to return that cash, with interest, in the future. In turn, financial institutions invest the funds with borrowers in exchange for the borrowers' promise to repay, with interest, at some future dates. Interest is the price paid or earned for the use of funds over time. The differential between interest paid and interest earned is the primary factor in determining the financial institution's profitability. Other sources of revenue are in the form of fees charged for services rendered such as bills collection, issuance of letters of credit, remittances and asset securitisation. As a result of the industry's competitiveness, more financial institutions are now not only keen to offer new financial products and services in line with meeting global and customers' expectations but to also tap developing or emerging markets in order to maximise wealth and profits.

In achieving this objective, financial institutions have to manage the risks inherent in the process of acquiring and investing funds because transactions give rise to assets, liabilities and commitments that represent the financial institutions' claims to receive and obligations to make future cash payments. Further, the exchanges financial institutions make, for most part, lack reciprocity, i.e., the financial institution may acquire funds from certain classes of customers on specific terms and conditions while in turn investing those funds with other classes of customers perhaps on different terms and conditions. The exchanges may also involve promises that the promisors may not be able to honour.

As a result of this lack of reciprocity, uncertainties expose financial institutions to risks. In addition, other factors that could subject financial institutions to risk include, among others, increased competition, pressure to operate in a profitable manner or to improve performance, introduction of new financial products and the rapid change in information technology. However, the risks inherent in the banking business can be mitigated if they are properly managed.

In this respect, internal auditors of financial institutions are expected to adopt a more dynamic rather than static audit approach. In addition to the routine checks and controls, internal auditors should assess their organisations' operating and financial risks and incorporate appropriate techniques and strategies in their audit process.

STUDENT PRACTICE 1

1. Other than the lack of reciprocity between acquiring funds and investing them, what other factors can also increase a financial institution's risks in its business? (para 1)

2. RISKS FACED BY THE BANKING INDUSTRY AND FINANCIAL INSTITUTIONS

2.1 Types of Risks

The increasing diversity and complexity of financial operations has seen various risks confronting the financial services industry. Certain new risk types emerge due to changes in methods of operations and/or innovations in products and services. Four main types of risks faced by financial institutions are listed below. They are by no means exhaustive and each risk type not mutually exclusive. Moreover, in a credit exposure, it is not only just credit risk but there are operational risks such as documentation risk where a financial institution is required to obtain proper documents, the sales and purchase agreement, and legal risks relating to perfection of legal documents.

a. Credit Risk

The risk of default by a borrower or counterparty, e.g. an issuer of a security held by the financial institution. Should a customer/counterparty default, financial institutions may face credit risk arising from significant loan write-offs especially when a loan is not properly collateralised. A sub-risk under this category is:

i. Collateral Risk

The risk associated with reduction in the value of collateral. For example, when a loan whose collateral is in the form of stocks and shares or a property depreciates in value, the financial institution will strive to obtain more collateral or request that the customer pledge more assets as collateral.

b. Market Risk

The risk of diminution or impairment in value of assets held, in particular, short-term liquid assets, due to adverse changes in market conditions attributed to the following sub-risks:

i. Liquidity Risk

This risk is associated with the demand for funds exceeding supply, i.e. when the bank is unable to fulfil its contractual obligations as they are due. It is further accentuated by the bank's difficulty in obtaining cash/funds at a reasonable cost through either the sale of its assets or new borrowings.

ii. Interest Rate Risk

The risk associated with interest rate movements in borrowing short to lend long. An increase in interest rates results in financial institutions having to increase the interest rates they pay on deposits without being able to invest at a higher rate until existing loans mature. High interest rate risk usually manifests itself through mismatches of maturities and durations between assets and liabilities.

iii. Foreign Exchange Rate Risk

The risk associated with movements in spot rates between two currencies where a financial institution's assets in one currency are matched by liabilities in another

currency. This risk arises as a result of sudden fluctuations in the foreign currency assets or liabilities held by the financial institution, and can affect the financial institution's income especially those involved in speculation.

c. Operational Risk

This risk is the exposure caused by deficiencies in the financial institution's information technology, business processes or internal controls that may result in unexpected losses. Operational risk may compound the effect of other risks. For example, although a loss may initially be due to credit risk, a breakdown of operational controls could cause the loss to grow much larger. For example, credit risks a financial institution faces may be further accentuated by instances of operational inefficiencies such as a non-performing loan account that is not properly monitored, misplacement of files and inappropriate legal action. Sub-risks under this category are:

i. Settlement Risk

The risk associated with failure to deliver payments or receipts in respect of exchange of foreign currency, financial instruments or commodities at maturity/termination.

ii. Legal and Documentation Risk

The risk associated with a lack of or insufficient documentation or protective clauses, which leaves the financial institution legally vulnerable. The institution can also face defamation suits as a result of wrongly returning a customer's cheque.

iii. Regulatory risk

This is the risk that a financial institution is unable to comply with the regulatory requirements expected of it and runs the risk of being penalised or reprimanded by the authority concerned. The news concerning its non-compliance could impair the institution's reputation.

iv. Reputation risk

This is manifested when a financial institution is unable to deliver what it promises in terms of its service and products. For instance, when it is unable to fulfil customers' cash withdrawals from their deposit accounts, its credibility or reputation as a sound financial institution is at stake

d. Strategic Risk

This risk encompasses the industry risk, concentration risk, reputation risk, disaster risk, regulatory risk, sovereign risk and social risk inherent in corporate strategy.

i. Capital Risk

This risk is closely tied to asset quality and the financial institution. The overall risk profile is dependent on the various types of loans given out to its customers, e.g. loans to government, other financial institutions, corporate customers and individuals. These loans are assigned a risk rating of 0% to 100% depending on

its risk profile as stipulated by BNM. The minimum requirement of an 8% capital adequacy ratio is calculated using the financial institution's capital base over its total risk-weighted assets.

ii. Industry risk

This is manifested in the form of trends/patterns affecting the financial services industry, such as the effect of globalisation.

iii. Concentration risk

This is manifested when a particular loan/asset portfolio of a financial institution is concentrated overly in one industry/market segment, etc. In the event the industry was to fail, the asset quality of the loans would be affected.

iv. Sovereign risk

This relates to a country's stability, which could be attributed to political and/or economic uncertainties. Hence, the level of risks increases when there is apparent turmoil or uncertainty in that particular country.

v. Catastrophic risk

These are events that have catastrophic impact, such as floods, a nationwide power interruption, etc.

Unless financial institutions identify all their risks, they will not be able to ascertain their exposures. While risks cannot be avoided, they can be minimised and managed by having appropriate controls and setting the organisation's risk appetite.

2.2 Critical Success Factors

The critical success factors of risk management depend on the following:

- a. Strategy,
- b. Organisation structure,
- c. Processes and feedback from business units to identify risk areas,
- d. Support from top level management, normally the board of directors, and
- e. Prioritising risks based on financial loss.

STUDENT PRACTICE 2

1. What are the main risks financial institutions face? (para 2.1)
2. What are the critical success factors of risk management? (para 2.3)

3. AUDIT OF CRITICAL OPERATIONAL AREAS

Internal auditors should focus their attention and direct their available resources to those operational units that entail significant risks that may have an adverse impact on the financial institutions' operations and financial conditions. The applicable operational areas deemed critical are identified in the BNM/GP10 as:

- a. branch operations,
- b. credit operations (lending),
- c. treasury operations (money market and foreign exchange),
- d. derivatives,
- e. investment in debt and equity securities,
- f. information technology, and
- g. insurance underwriting and insurance claims.

STUDENT PRACTICE 3

1. What are the critical areas of operations that internal auditors should focus on? (para 3)

4. BRANCH OPERATIONS

Branch operations refer to the business and operational acts undertaken by a branch of a financial institution. When a financial institution has many branches, auditors must consider a number of factors when determining their audit approach to provide assurance to management as follows:

4.1 Scope of Audit

The branch audit should include a review of the branch's performance in addition to the audit of the branch's compliance with the internal and regulatory guidelines and other legal requirements.

4.2 Internal Auditors' Role in Branch Operations

The auditable areas in a branch will include:

- a. Credit review of loans and advances,

Refers to the review of branch's credit processing. Auditors should assess the credit decisions the branch makes when approving credit applications to ensure they are consistent with head office policies.

- b. Review of branch's performance in terms of the following:
 - i) Asset Quality
 - Analysis of the portfolio of loans,
 - Review of utilisation of facilities granted,
 - Loan delinquency and non-performance loans, and

- Adequacy of specific and general provisions for bad and doubtful debts.
- ii) Deposits
 - Structure of deposits, and
 - Loans to deposits ratio.
 - iii) Other services
 - Bank-related services, e.g. remittances, bill collection services and safe-deposit operations,
 - Channel and distribution services such as electronic banking, and
 - Customer service issues.
 - iv) Profitability
 - Earnings,
 - Cost income ratio,
 - Loan margin,
 - Cost of funds, and
 - Achievement of budget and other key performance indicators.
- c. Review of compliance with operational procedures and accounting controls,
 - d. Review of the validity and accuracy of financial records and management reporting, and
 - e. An overall review of branch's management procedures.

Internal auditors should assess the effectiveness of organisational and management controls exercised by the head office and obtain reasonable assurance that the branch's procedural controls are operating effectively. Particular attention should be given to the smaller branches where low staff levels or lack of staff competencies makes it more difficult to ensure adequate segregation of duties.

STUDENT PRACTICE 4

1. Identify the auditable areas when carrying out a branch audit. (para 4.2)

5. CREDIT OPERATIONS (LENDING)

Credit operations involve credit appraisal, approval, documentation, disbursement, supervision, recovery and rehabilitation. There are generally four stages in the lending process, as follows:

Stage I - Marketing

This involves identifying and calling upon potential and existing borrowers.

Stage II - Credit Processing

This involves verification, checking customers' credit background through the CTOS or CCRIS, credit analysis and the acceptance/rejection of loans/proposals.

Stage III - Legal/Payment

This involves processing of legal documentation and disbursements.

Stage IV - Asset Management

This involves monitoring the loans portfolio, portfolio analysis and problem evaluation.

In most financial institutions, loans and advances usually account for a significant proportion of assets, and contribute a substantial portion to total revenue. Therefore, the risk associated with credit operations is crucial and has to be properly addressed and managed.

5.1 Risks Inherent in Credit Operations

Internal auditors should assess whether their financial institutions have dealt adequately with borrowers' credit risk profiles in their credit policy and procedures. The credit policy should address the types of customers (market segment, industry, etc) and loan products that the financial institution is willing to lend. This reduces the possibility of default, fraud or insolvency risks. The internal auditors should also take cognizance of the requirements of the various guidelines issued by BNM, such as BNM/GP5: Guidelines on the Credit Limit to a Single Customer and BNM/GP6: Guidelines on Credit Transactions and Exposures with Connected Parties. These guidelines are discussed in more detail in Chapter 4.

Listed below are some of the risks associated with credit operations. There maybe more risks than the six types of risks highlighted:

a. Credit Risk

The borrower's credit-worthiness, his capacity to repay and other financial credentials/dealings are the most significant risks involved in credit operations. His repayment capabilities may be affected by general economic conditions, interest rate levels, unemployment and downturns in particular economic sectors, and market conditions. In addition, changes in the business' constitution or ownership may also affect credit risk.

In lending, there are five credit factors to consider when evaluating a credit proposal. Popularly known as the 5Cs, they are Character, Capability, Condition, Capital and Collateral. **Character** is said to be that quality in a borrower that makes him want to repay when a debt is due. Factors that contribute toward a borrower's character are honesty, responsibility, attitude and virtuousness. **Capability** is defined as the borrower's ability to repay his loan. This is generally represented by the borrower's income.

Meanwhile, **Capital** represents the borrower's money put into a project or business. The amount of capital reflects his commitment to the project. This capital provides the borrower with the ability to absorb a certain amount of loss. Financial institutions must also consider the following in the situation in which the borrower operates, when doing the assessment – economic conditions, industry outlook and government policy. **Collateral** is self-explanatory.

Under the Basel II Accord, it is recommended that financial institutions develop an internal credit risk rating system for corporate and business loans. The rating system should be comprehensive as well as consistent with the nature, size and complexity of a financial institution's activities. The credit risk rating system should be detailed in the credit policy and procedures developed for the determination of credit grades, and subject to periodic review. Financial institutions should regularly monitor and evaluate the actual default or loss experience of credits in each risk grade as a means of assessing the consistency and reliability of the ratings being used.

b. Collateral Risk

The continual adequacy and quality of legal security is important as they post the last avenue for recovery of outstanding debts in the event a borrower defaults on his repayment. The maintenance and reduction in value of the collateral offered should be assessed periodically. Collateral should also be adequately insured, and its forced sale value and ability for conversion to cash should be valued by the financial institution's panel of valuers on a regular basis to obtain the actual market value of the property pledged as collateral.

c. Documentation Risk

The credit facility should be documented properly to protect the financial institution's interests if it is necessary to take legal action against the borrower or guarantor. For example, loan agreements should be stamped and signed under seal, and corporate resolutions should be obtained when lending to corporations.

d. Sovereign Risk

When a financial institution lends to borrowers in a different country, it is also exposed to the country risk of payment default caused by changes in political policies as well as its laws and the legal system.

e. Operational Risk

Once a borrower accepts the credit, the account should be managed carefully to minimise the risk of any losses being incurred as a result of human error, poor communication among employees and supervisors, lack of understanding, unauthorised activity, inadequate monitoring and system breakdowns, or loss of documents.

f. Strategic Risk

The credit facilities a financial institution grants should be in line with its strategy.

5.2 Credit Risk Management

A financial institution's exposure to risks can be minimised through supervision and controls over the extension of credit, risk exposure to the various economic sectors, close credit monitoring and evaluation of collateral. Furthermore, its credit strategy, policies and risk management will affect the quality of loans and advances.

a. Credit Strategy

The financial institution's credit strategy includes the organisation's defined objectives and goals for extending credit facilities so as to achieve profitable returns while assuming the risk appetite 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 rate margins and fees, and identify the risk parameters. Internal auditors should ensure that the credit strategy and policies are in compliance with the guidelines set by management and approved by the board.

b. Policies and Procedures

Credit policies and procedures usually provide detailed guidelines for credit appraisal and administration. These include all large credit exposures granted to individual borrowers or a single group of borrowers. They must be reviewed regularly at least once a year and reported to management on a monthly basis.

Internal auditors should address the following areas of audit concern:

- i) Credit policies and procedures are adequate and updated with the latest innovative products;
- ii) Credit operations are in line with the approved credit strategy, policies and procedures;
- iii) Proper segregation of duties and responsibilities relating to loan processing, loan approval, custody of security and legal documents as well as loan administration;
- iv) Borrowers' creditworthiness and repayment capacity are carefully appraised and evaluated prior to approval of credit facilities;
- v) Credit disbursements are made only after security and legal documentation have been duly completed;
- vi) An effective system is in place for credit monitoring, supervision, recovery, accounting and financial reporting;
- vii) No over-concentration of credit to a particular borrower;
- viii) Management review of credit exposures to borrowers is carried out periodically and in a timely manner;
- ix) No credit facilities are granted to director-interest companies for self-serving purposes. This involves credit facilities to nominees of the directors and officers of the financial institution; and
- x) Loan information and correspondence are properly maintained in the credit file.

c. Security and Legal Documentation

It is pertinent that security documents are duly executed, validated and lodged with the relevant authorities. In addition, the storage and retrieval of these documents must be recorded under adequate custody with proper segregation of incompatible functions.

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

- i) The financial institution's beneficiary rights to collateral have been duly registered with the authorities to ensure its enforceability in the event of default;
- ii) Procedures relating to safekeeping of and control over the access to security documents and proper maintenance of collateral records are adequate;
- iii) Security and loan documentation are undertaken by the financial institution's panel of lawyers;
- iv) Appraisal of value of landed security is undertaken by the financial institution's panel of valuers or other approved valuers; and
- v) Procedures concerning withdrawal, substitution and discharge of collateral are in place and being adhered to.

d. Credit Disbursement

A pre-disbursement checklist is signed off to ensure that all security and legal documentation is in order and complete, and conditions precedent are fulfilled before disbursement of credit.

Internal auditors should address the following areas of audit concern:

- i) Pre-disbursement checklist is duly signed off by the loan administration officer and approved by the relevant authority before loan proceeds are released to borrowers; and
- ii) Loan proceeds are released in accordance with the approved terms and conditions.

e. Credit Monitoring, Supervision and Recovery

An effective credit review/monitoring system includes analysing the borrower's periodic financial statements and financing requirements, reassessing collateral values, making site visits to the borrower's business premises and keeping abreast with trends and developments in the industry. In the event that credit facilities turn into non-performance loans (NPLs), an effective credit recovery system is pursued to minimise loan losses.

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

- i) Collateral is valued periodically to ensure that credit exposures are within the margin of advance;
- ii) Potential delinquent loans are identified in a timely manner and prompt follow-up measures adopted;

- iii) Management is informed of the status of delinquent loans;
- iv) Adequate review of all borrowers' existing credit facilities are carried out regularly with the view to renew, enhance, reduce or restructure the credit facilities;
- v) Borrowers are appropriately graded in relation to risks; and
- vi) Restructured/rehabilitated loan accounts are properly approved and closely monitored.

f. Accounting and Financial Reporting

It is management's responsibility to establish a proper accounting and financial reporting system on the various credit facilities approved.

Internal auditors should address the following areas:

- i) Loans are properly accounted for, correctly stated, classified and disclosed;
- ii) Reports on credit information to management and the board are relevant, accurate, adequate and timely. These include analyses of loan profiles, loan growth, income contribution and concentration of credits in relation to economic sectors and borrowers;
- iii) Balances of subsidiary loan records should tally with the amount stated in the general ledger. Reconciliation should be current and immediate action taken to resolve any differences. The reconciliation should be reviewed and approved by the appropriate supervisory personnel;
- iv) Pertinent loan information (e.g. bumiputera/non-bumiputera, resident controlled status and economic sectors) is promptly recorded and independently verified to ensure accuracy;
- v) Adequate systems are in place to ensure that the credit exposures reported in the management accounts and BNM statistical returns are correctly stated; and
- vi) Accounting policies on income recognition, provision for loan losses and suspension of interest on non-performing loans are consistently applied.

g. Legal and Regulatory Requirements

Management is responsible for ensuring that credit facilities granted to borrowers do not breach any provisions of the BAFIA, Islamic Banking Act, Insurance Act, Takaful Act, BNM directives and guidelines issued from time to time, and other laws and regulations.

Internal auditors should review the financial institution's compliance with legal and regulatory requirements, in particular, the following:

- i) Loans and advances are not granted against the security of the financial institution's own shares;
- ii) Unsecured credits are extended in compliance with the provisions of the BAFIA;
- iii) Credit is not extended in excess of the single customer limit imposed by BNM;

- iv) No extension of credit to directors, staff and their interested concerns other than those permitted under the BAFIA;
- v) No approval of credit facilities in excess of the credit officers' discretionary limits; and
- vi) No extension of loans beyond the threshold limit imposed by BNM from time to time, e.g. loans secured against shares and units in unit trusts.

Internal auditors should also ascertain whether there is an adequate system in place to ensure the following:

- i) Classification and suspension of interest on non-performing loans and provisions for bad and doubtful debts are in compliance with the minimum requirements of the BNM/GP3: Guidelines on the Suspension of Interest on Non-Performing Loans and Provision for Bad and Doubtful Debts;
- ii) Credit facilities are classified correctly for the computation of the risk-weighted capital adequacy ratio;
- iii) All large credit exposures are promptly and accurately reported to BNM;
- iv) Reported data is accurate and reliable before it is submitted in diskette media to BNM in conjunction with the third quarter review on the adequacy of provision for bad and doubtful debts;
- v) Loans to priority sectors and non-residents are correctly classified and reported; and
- vi) Statistical information in relation to credit facilities are correctly reported and submitted to BNM.

5.3 Internal Auditors' Role in Credit Risk Management

Internal auditors should ensure that their financial institution has an internal control system to appraise loan exposures and to assess the quality of the various assets. Based on the "Best Practices for the Management of Credit Risk" issued by BNM on 1 September 2001, financial institutions should establish an independent committee known as the Credit Risk Management Committee. The responsibilities of the committee include the following:

- a. evaluate and assess the adequacy of strategies to manage the overall credit risk associated with the financial institution's activities;
- b. oversee the formal development of credit policies within the financial institution, encompassing all products and businesses and ensuring the development of a policy manual and procedures;
- c. monitor, assess and advise on the financial institution's credit risk portfolio composition;
- d. evaluate risks under stress scenarios and the capacity of the banking institution's capital to sustain such risk;
- e. assess the risk-return trade-off;
- f. review the credit review process and asset quality reports, and ensure that corrective action is taken; and

- g. review and evaluate the various credit products engaged by the financial institution to ensure that it is conducted within the policies set by the board.

Financial institutions should also establish a separate credit review (audit) department staffed by experienced, independent credit analysts to conduct post-reviews on credits that have been approved and provide independent judgements on the quality of both the credit appraisals and the financial institution's credit portfolio.

During audit planning, an internal auditor should study the loan portfolio and perform a risk assessment of credit operations before formulating the audit objectives and scope. The more important audit areas to look at in credit operations include:

- a. approval levels,
- b. collateral types,
- c. margin of financing in relation to risks, i.e. the higher the risk, the higher the margin to compensate for default,
- d. compliance with statutory guidelines and internal policies,
- e. interest computation, especially when there is a change in specifications in computer applications programs,
- f. accuracy and completeness of reports to management, and
- g. quality of credit reviews.

5.4 Methodologies to Study the Loan Portfolio

The following methodologies can be applied to study the loan portfolio:

- a. risk assessment models;
- b. computer-assisted audit tools/technologies;
- c. internal control questionnaire;
- d. results of past audits; and
- e. ad hoc triggers.

5.5 Risk Evaluation

In risk evaluation, credit proposals for commercial loans in particular should address the following aspects:

a. Purpose and Structure of the Credit

- i) Is the purpose clearly defined?
- ii) Are there any existing debts being replaced by the proposed credit?
- iii) Are there any credit facilities with the financial institution, i.e. any possibility of cross default?
- iv) Organisation structure of the company as well as its group of companies.

b. Qualitative Factors

- i) Maturity of the industry, i.e. infant or declining;
- ii) Vulnerability of the industry, i.e. high technology, cyclical;
- iii) Market position of borrower;
- iv) Susceptibility to government policies, foreign currency;
- v) Concentration of customers and suppliers;
- vi) Competence and experience to cope with challenges and changes;
- vii) Structure and ability to support future growth; and
- viii) Capacity of capital assets such as plant and machinery.

c. Quantitative Factors

- i) Financials and ratio analysis;
- ii) Working capital and liquidity; and
- iii) Borrowing structure, i.e. are sources matched with needs or long-term needs being met from short-term sources?

d. Risk and Return

- i) Factors that influence the return required from the loan; and
- ii) Factors that contribute to the return on the loan.

e. Credit Limits

Credit limits should be established for each counterparty based on the type of transactions, assessment of the counterparty's creditworthiness and expected utilisation of the facility.

5.6 Authority Limit

Under section 65(1) of the BAFIA, a director or an officer of a licensed institution is prohibited from granting any credit facility in excess of his authority limit, or outside the scope of any terms and conditions, imposed on him by the licensed institution, or in contravention of any directions given to him, or any agreement made with him by the licensed institution.

A director or an officer who contravenes this provision is liable to imprisonment of up to 5 years or a fine of RM5 million, or both.

It is, therefore, important that a director or an officer be made aware and familiar with the parameters of their respective lending limits and authority. For instance, no credit facility can exceed its sanctioned limit before such approval is first obtained from the relevant authority. This is common in the granting of unsecured loans or exceeding the margin requirements for loans against shares or the overdrawn of temporary overdraft facilities.

(Source: Extracted from *Module 1 – Regulatory Framework, CCP Study Manual, July 2003, p 3-17*)

5.7 Monitoring of Borrowers' Accounts

The close monitoring of borrowers' accounts will help to identify potential non-repayment early so that the problem can be addressed. The following are some of the common early warning signs:

a. Business

- i) Unplanned divestitures,
- ii) Unplanned growth or diversification,
- iii) Cash draining subsidiaries,
- iv) Loss of market share,
- v) Product litigation,
- vi) Unknown effect of labour issues,
- vii) Failure to maintain capital, research or development expenditure, and
- viii) Over reliance on a single product or customer.

b. Financial

- i) Adverse trends in sales and earnings,
- ii) Results differ from budget,
- iii) Interim losses,
- iv) Poor liquidity,
- v) Collection from customers off plan,
- vi) Unusual borrowing pattern,
- vii) Qualified audit report,
- viii) Diversion of funds, and
- ix) Breaches in loan covenants.

c. Industry

- i) Excess capacity,
- ii) Deregulation,
- iii) Changes in policies,
- iv) Product subject to intense competition,
- v) Poor position in industry, and
- vi) Failure to keep pace with changes in technologies.

d. Management

- i) Weak performers,
- ii) High staff turnover, and
- iii) Departure of key management staff.

e. External

- i) Stock market,
- ii) Trade inquiries,
- iii) Devaluation, especially where there is a dependence on imports from countries that have strong currencies, and
- iv) Adverse regulatory, political or economic environment.

5.8 Key Ratios to Measure Lending Risk

The **key ratios** to measure lending risk are:

- a. Doubtful debts: gross loans, and
- b. Loans provision: non-performing loans.

If asset quality is poor, a financial institution needs a large reserve in terms of specific and general provisions because it might need to charge off such loans.

5.9 Success Factors

The following are success factors in assessing the monitoring of risks in the credit operations:

- a. Improving credit quality,
- b. Minimise loan losses,
- c. Strong proactive credit management,
- d. Proper balance between loan quality and growth,
- e. Effective credit policies and clear operational procedures,
- f. Appropriate credit structures, and
- g. Effective management information system.

STUDENT PRACTICE 5

1. What are the inherent risks faced in credit operations? (para 5.1(a) to (f))
2. What are some of the ways to ensure credit policies are effective? (para 5.2 (b))
3. What should an internal auditor do to protect the bank's interest against the inherent risks of a credit operation? (para 5.2 (a) to (g))
4. What are some of the responsibilities of a CRM Committee as outlined in the BNM guidelines? (para 5.3)
5. Name three qualitative factors when evaluating a commercial loan proposal. (para 5.5(b))
6. What are the two key ratios in measuring lending risk? (para 5.8)

6. TREASURY OPERATIONS (MONEY MARKET AND FOREIGN EXCHANGE)

Deposits and other borrowings are the primary source of funds a financial institution uses to fund loans and investments. It must strike a balance between the potentially conflicting principles of the need to make a reasonable return on its loans and to ensure the obligation it owes to its depositors.

The function of a financial institution's Treasury Department is to carry out foreign exchange (FX) and money market (MM) transactions. FX transactions cover commercial deals arising out of international trade, money transfers and foreign investments. MM operations cover both short-term borrowing and lending activities as well as trading of financial papers or instruments.

6.1 Risk Associated with Treasury Operations

Internal auditors should evaluate whether the designed internal control system is capable of identifying, monitoring and managing the major risks associated with treasury operations.

The major risks associated with treasury operations are:

a. Foreign Exchange Risk

If a financial institution's assets in one currency are matched with liabilities in another currency, it is exposed to foreign exchange risk due to movements in the spot exchange rates between the two currencies. The most important measure of exchange rate risk is the net open position, which is the net of the spot and forward positions of both assets and liabilities.

b. Interest Rate Risk

An exposure to interest rate movements arises most obviously, when the financial institution borrows short-term money and lends at a higher rate for a longer period. If the interest rate rises, the financial institution will have to raise the interest rate it pays on deposits, without being able to invest at higher rates until the existing loan matures. For example, if a financial institution has borrowed money for 1 month at a fixed rate and lent it for 6 months also at a fixed rate, it will need to acquire new funding after 1 month to finance the loan for the remaining 5 months. If the market interest rate has risen higher than the interest rate of the loan, the financial institution may lose money for the remaining 5 months because it has a commitment to continue lending the loan at the fixed rate while having to obtain new deposits at a higher rate. This exposure is called interest rate risk.

c. Credit Risk

When the Treasury Department places funds with other financial institutions (i.e. interbank placements), the financial institution is exposed to the same credit risk faced by its Credit Department's lending. In fact, the Treasury Department's credit risk is especially vital because interbank placements are not collateralised. Under extreme market conditions, the financial institution's failure to repay will trigger a systemic risk in the banking industry.

d. Liquidity Risk

There are two important aspects to liquidity. Firstly, liquidity means the financial institution has access to cash when needed and is able to obtain the required cash to meet any unforeseen requirement at any time and at a reasonable prevailing market rate. Secondly, liquidity also means that the financial institution owns assets/instruments (whether for trading or investment purposes) that can be easily converted into cash as and when required and at not too great a cost. Hence, the liquidity risk the financial institution faces is the risk of not being able to fund its own position.

Financial institutions always face the uncertainty that depositors may withdraw their deposits anytime and they have a duty to pay the depositors. Thus, if a financial institution uses short-term funds (i.e. borrowing “short”) to invest in long-term assets (i.e. lending “long”), there is a risk that if depositors withdraw their money, it may be unable to convert its long-term assets, e.g. loans into cash, to meet its obligations. It also may not be easy to borrow temporary funds at a reasonable price from the interbank market. The financial institution may have to pay a higher interest rate than the prevailing market rate, and turn to BNM to satisfy its immediate liquidity needs. On the other hand, having too much liquidity is a disadvantage because the financial institution will have to pay interest on these funds while not utilising them to generate income.

e. Sovereign Risk

When a financial institution places funds with other financial institutions at different locations outside Malaysia, it is exposed to the risk of payment default caused by changes in the political policies of those countries. Thus, lending money to branches of the same bank located in different countries can result in country risk, i.e. exposure to nationalisation, non-repatriation of profits, etc.

f. Operational Risk

Operational risk is similar to that for lending operations. Once a transaction is contracted, it should be managed carefully to minimise the risk that losses may be incurred as a result of human error, poor communication, lack of understanding, unauthorised activities, inadequate monitoring and system breakdowns.

g. Settlement Risk

When a financial institution invests in securities, it is exposed to settlement risks that the borrower may not remit the funds on the maturity date. To reduce such risks, it may wish to consider capping settlement on maturity of instruments by currency and tenor to each counterparty.

h. Strategic Risk

The composition of a financial institution’s assets and liabilities should be aligned with its funding strategy.

i. Capital Risk

In managing its profile to mitigate capital risk, a financial institution should also ensure that its assets are of good quality. This has an effect on its capital adequacy ratio.

6.2 Internal Auditors' Role in Treasury Operation Risk Management

Financial institutions are expected to mitigate risks while maximising profits to ensure that they are able to raise funds and meet payment obligations in a cost-effective manner. Hence, internal auditors may also wish to evaluate their organisations' documented liquidity contingency plan to ensure its adequacy.

Funding loans with liabilities of comparable maturity and rate sensitivity is one of the key strategies to control risks, i.e. matching cashflows and maturity profiles of assets and liabilities. A financial institution can either adopt a "match" or "mismatch" asset/liability portfolio. A "match" book is whereby the dealer matches assets and liabilities on a transaction-by-transaction basis. For example, if the institution takes a 1-month deposit, it will also lend the deposit for 1 month, hence locking up the margin between the deposit and placement for 1 month. In this case, there is no gap position for the dealer to take advantage of interest rate movements to generate more income.

Internal auditors should ensure that their financial institutions have in place an internal control system to regularly monitor the gap position to assess the impact on the institution's assets and liabilities profiles. The results should be evaluated against the organisation's funding and lending strategy.

a. Policies and Procedures

The treasury policies should be consistent with the financial institution's business strategies, capital strength and management expertise. The policies should also specify the organisation's risk appetite, i.e. its overall willingness to take risks. Normally, the board of directors approves the treasury policies, which should be clear and comprehensive with regular updates to reflect changes in market practices, economic conditions and regulatory compliance.

Board policies should also include trading objectives and strategies, management control and supervision of FX and MM activities, approved list of brokers, approving authorities and discretionary limits, operational and counterparty limits and trading hours outside normal business and off-premises dealings. The procedures should cover settlement, extension and cancellation of contracts, giving of preferential rates, approval and duration for excesses, and detailed descriptions of accounting, revaluation and reconciliation processes.

Internal auditors should address the following areas of audit concern:

- i) Adequacy of and compliance with established policies and procedures;
- ii) Treasury operations are in line with the asset and liability management committee's objectives and strategies;
- iii) Proper practice of segregation of duties and responsibilities relating to the dealing, processing, settlement, accounting, revaluation and reconciliation functions;

- iv) Adequacy of and compliance with internally approved trading limits;
- v) Amendments made to contracts, if any, are properly authenticated;
- vi) Inward and outward confirmations are verified and matched. Discrepancies are checked immediately with the counterparties and recorded in the log book, and any unusual or irregular transactions are investigated;
- vii) Dealing positions of foreign branches and other related offices are adequately monitored;
- viii) Perform independent revaluation of foreign currency accounts on a periodic basis;
- ix) Settlements of FX and MM transactions are in accordance with instructions stipulated in the contracts;
- x) Proper controls over fund transfers either through RENTAS or SWIFT, and transfers of ownership of debt securities are issued through the Scripless Securities Trading System (SSTS);
- xi) Internal auditors should be alert to transactions which are exceptional or highly speculative in nature; and
- xii) Experience, training and performance tracking of all traders/dealers.

b. Assets and Liabilities Management (ALM)

Balancing assets, liabilities and profit as well as managing the risks require some anticipation of future economic conditions and their likely impact on the financial institution's funding and investment alternatives. Should an unfavourable set of circumstances occur, the financial institution may need to examine the impact on profits. However, a too cautious strategy may also lead to loss of opportunity against its competitors who have taken greater risks with better anticipation of the environment.

Thus, it is of paramount importance that financial institutions manage their assets/liabilities strategies for profit, and such responsibilities should not rest on a single decision-maker. Internal auditors should ensure that the organisation has an effective Asset and Liability Committee (ALCO) to develop asset/liability management strategies so as to maintain the required funding and liquidity exposures within the acceptable threshold (risk limits) as approved by the board of directors. The ALCO should know its asset/liability mix, anticipate present and future liquidity requirements and review scenario analysis with the operating personnel to formulate the best strategies. These may include hedging and contingency funding as part of the overall strategies.

ALM includes interest rate management, liquidity management, and assets and liabilities maturity matching. In this respect, ALM deals with strategic issues such as the structure of the balance sheet, proportion of capital to total assets, quality of earnings and maintenance of liquidity requirements.

Internal auditors should review the system used by ALM in managing risks associated with FX and MM transactions. This may include a review of past performance to assess the profitability and liquidity of the financial institution's asset and liability structure in response to interest rate sensitivity, interest re-pricing and the 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.

c. Accounting and Financial Reporting

In reviewing the accounting system of treasury operations, internal auditors should determine whether:

- i) recording, revaluation and income recognition of FX and MM transactions are carried out promptly and in accordance with approved accounting standards;
- ii) accounting records are adequate for preparing position reports and for evaluating FX positions; and
- iii) reconciliation of all nostro accounts is performed frequently and all unreconciled items are resolved in a timely manner.

Internal auditors should also assess the reliability of the system used to generate management reports and BNM's statistical returns.

d. Legal and Regulatory Requirements

Internal auditors should review compliance with legal and regulatory requirements, particularly the following:

- i) Repo transactions are properly accounted for;
- ii) The net FX open position is at all times within the limit set by BNM;
- iii) Proper classification of FX transactions into trade and non-trade categories;
- iv) Proper classification of FX transactions for the purpose of capital adequacy requirements; and
- v) The Code of Ethics and Code of Conduct issued by the Persatuan Pasaran Kewangan Malaysia and BNM respectively are complied with.
- vi) Dealers who are authorised to trade on the financial institution's behalf have passed the necessary examinations of the relevant bodies such as the Persatuan Pasaran Kewangan Malaysia or the Securities Commission.

6.3 Managing Liquidity Positions

The financial institution's liquidity position in respect of any determined period may be measured by the total receipts due less total payments due during that period. In doing so, it should take into consideration the following factors to reflect a realistic liquid position:

- a. The determination of the earliest repayment date. It may be misleading, although prudent, to use the earliest repayment dates for all liabilities, especially if the financial institution has a significant amount of demand liabilities (as this might show an unrealistic "worst case" position and permanent liquidity). Therefore, it may need to assume a proportion of its liabilities at earliest repayment date in the calculation of the liquidity position;
- b. Commitments to make funds available on a particular date in respect of maturity of deposits and drawdown of approved credit lines by borrowers;

- c. Realisability of marketable securities, i.e. how quickly the securities can be disposed of for cash in the event of a forced sale and the discounts offered, i.e. loss of opportunity gain; and
- d. Standby facilities available from other financial institutions.

6.4 Other Important Measures in Minimising Risks

The risks should also be minimised by having the following measures in place:

- a. Mark to market all off-balance sheet items;
- b. Set limit exposures to control the extent of exposures to which the financial institution is vulnerable;
- c. Diversify exposures, e.g. in terms of customer base and to control growth without violating exposure limits; and
- d. Maintain flexibility of strategies so that the financial institution can respond to changes in economic conditions that have a negative impact on its position.

The key ratios for monitoring liquidity risks are:

- a. Core deposits*:Gross loans, and
- b. Equity:Assets.

* Core deposits are deposits that are considered stable and not highly interest rate sensitive.

6.5 Management Information System

The financial institution's management information system should be able to provide the following services:

- a. Managing liquidity and interest rate risks;
- b. Evaluating the quality of treasury assets;
- c. Foreseeing implications or impact of changes in the mix of assets and liabilities;
- d. Having insights into current and future cost of funds;
- e. Analysing future cashflows and liquidity needs; and
- f. Ensuring the financial institution complies with statutory requirements and internal policy.

STUDENT PRACTICE 6

1. Give five major risks associated with treasury operations. (para 6.1(a) to (i))
2. What are the two important aspects of liquidity? (para 6.1(d))
3. What are the main responsibilities of an ALM Committee? (para 6.2(b))
4. What are the areas of focus when reviewing the accounting system of treasury operations? (para 6.2(c))

7. DERIVATIVES

Financial institutions can use derivative products to manage risks by controlling exposure and reducing funding costs and foreign exchange fluctuations, along with other tax and accounting advantages by adjusting the timing, amount and predictability of cashflows. A derivative is simply a transaction or contract, whose value depends on, or derives from, the value of an underlying asset or index. Examples of derivatives are currency options, interest rate swaps, cross-currency swaps and index futures.

One party with exposure to unwanted risk can pass some or all of that risk to a second party. The first party can assume a different risk from the second party, pay the second party to assume the risk or create a combination. For instance, in an interest rate swap, counterparty A who has a fixed rate asset may not wish to be exposed to interest rate risk in the event of a hike in interest rates. Hence, counterparty A could transact with counterparty B in an interest rate swap whereby counterparty B may absorb the fixed rate exposure and counterparty A will, in turn, receive a floating rate income arising from the asset. In order for such a transaction to occur, both parties must have differing views on the interest rates outlook.

However, without a control system to manage risks that give rise to unpredictability of cashflow, these risks have the potential to cause significant financial losses. For example, on 26 February 1995, Barings collapsed due to a lack of fundamental internal controls such as lack of proper segregation of duties between the dealing room and back-office. Unauthorised tradings were, therefore, not detected. A single trader, 28-year-old Nick Leeson, lost \$1.3 billion from derivatives trading. The loss wiped out the firm's entire equity capital. Leeson accumulated a position of \$7 billion in stock index futures on the Nikkei 225. However, this enormous transaction was not reported to the management due to poor back-office controls. As losses mounted because of a more than 15% fall in the market, Leeson increased the size of his positions in a stubborn belief that he was right. The increase in his exposure was not detected. Unable to meet the margin call, Leeson simply walked away, leading to the collapse of Barings.

There are minimum standards on Risk Management Practices for Derivatives pertaining to financial institutions' derivative operations. To carry out their audit effectively, internal auditors must be well conversant and knowledgeable in derivative products and transactions, and familiar with the relevant regulations and guidelines governing derivative activities in order to evaluate the financial institutions' compliance.

7.1 Risks Inherent in Derivative Products

Risks inherent in derivatives include market, credit, operational, liquidity and legal risks. The nature and types of derivative products transacted will dictate the level and amount of risk that a financial institution is prepared to assume.

The more significant risks encountered when using derivative products are set out below:

a. Market Risk

Market risk is associated with unfavourable changes in the market price of the derivative instrument resulting from movements in currency exchange rates, interest rates, commodity and equity markets as well as the time value and volatility of the market of the underlying instruments.

b. Credit Risk

Credit risk for derivatives is the same as that faced by the credit (lending) department. The risk of one counterparty defaulting on its obligation can cause a ripple and a catastrophic effect on the financial system.

c. Liquidity Risk

Liquidity risk for derivatives concerns the risk that the instrument may not be easily liquidated at the market price.

d. Operational Risk

Derivatives, like other money market instruments, create operational risks once the transaction is contracted. The transaction should be managed carefully to minimise the risk of incurring losses as a result of human errors, poor communication, lack of understanding, unauthorised activity, inadequate monitoring and system breakdowns which lead to inaccurate accounting and record-keeping, fraud, incorrect market valuation and failure to settle.

7.2 Internal Auditors' Role in the Internal Risk Management System of Derivatives

Internal auditors should ensure that financial institutions have in place an internal risk management system to control and monitor risks. As with other business operations, management must identify the risks for derivatives through a full understanding of the products.

Every financial institution should establish its risk appetite for the risks identified, i.e. the level of risks it is prepared to assume. The risk appetite and risk management objectives should be clearly defined through policies approved by the board of directors. As with money market operations, strategies should be developed and reviewed by a committee such as the ALCO.

With a system for risk identification in place, it is critical for financial institutions to measure risk by focusing on both accounting and market value. The risk measurement system should constantly be verified through the segregation of duties and implementation of input and reconciliation controls. The system should periodically carry out a stress-test or simulate the impact of changes on the value of the entire portfolio.

Internal auditors should assess whether their financial institutions' risk exposures have either become too excessive vis-à-vis their respective capital positions or have not been timely identified to the extent that they represent unsafe and unsound banking practices.

In this manner, internal auditors should:

- a. Review whether the financial institution has complied with the requirements on common integration of risks, measurement, limits and reporting, and management evaluation and supervision;
- b. Conduct periodic reviews of the risk management models used;

- c. Ascertain whether management and the officers involved in derivative operations are fully aware of the risks associated with all on- and off-balance sheet transactions. In addition, whether such transactions are carried out for hedging or speculative purposes;
- d. Determine whether management has exercised caution when the financial institution is involved in over-the-counter derivative transactions. They should look into aspects such as the nature and types of derivative products, why and how they are transacted and whether they dictate the level and amount of risk that the financial institution is prepared to assume.

7.2.1 Policies and Procedures

The financial institution should have written policies and procedures on derivative operations that will include parameters on risk activities, types of derivative products traded, approving authorities and discretionary limits, review of various operational and counterparty limits, and a list of authorised traders.

These policies and procedures should cover:

- a. Organisational structure and job responsibilities;
- b. Reporting requirements;
- c. Monitoring and stop-loss mechanisms;
- d. Permissible activities; approved list of brokers and counterparties;
- e. Dealing guidelines (including off-market transactions and off-premises dealings);
- f. Pricing assumptions, model and mechanism;
- g. Dispute resolution methodology;
- h. A detailed description of transaction processes; and
- i. Settlement, accounting, revaluation and reconciliation procedures.

With respect to the above, internal auditors should review their financial institutions' compliance in the following significant areas:

- a. All significant policies relating to management of derivative risks must be approved by the board and should be consistent with the organisation's approved business strategies, capital strength, management expertise and overall willingness to take risks;
- b. Management, in carrying out the approved policies, should ensure there are adequate operational guidelines and procedures in place for conducting derivative operations vis-à-vis long-range and on a day-to-day basis. This should include:
 - i) A clear delineation of lines of responsibility for managing risks;
 - ii) An effective system for measuring risks;
 - iii) A comprehensive risk-reporting process;
 - iv) Appropriate limits on risk-taking;

- v) Adequate dealing, processing and settlement procedures and an effective system of internal control;
 - vi) Effective monitoring and enforcement at all levels of management;
 - vii) Sufficient resources and competence to carry out daily operation and risk management functions effectively;
 - viii) Adequate revaluation procedures for derivative transactions; and
 - ix) Adequate pricing models or mechanisms for derivatives.
- c. A committee is set up to approve, oversee and control derivative activities;
 - d. An independent research unit is set up to monitor and ensure that derivative activities are conducted within the established policies and guidelines and to conduct research and recommend improved risk measurement methods and control procedures;
 - e. Development of risk policy and the process of measuring, monitoring and controlling risk should be performed independently of individuals conducting derivative activities (marketing, dealing and processing);
 - f. New derivative activities should be avoided until management has acknowledged and fully understood the activity, and is in a position to oversee and manage the new activities; and
 - g. Customers are offered derivatives for purposes of hedging only, and an adequate assessment on the suitability of the derivative products being offered.

7.2.2 Accounting and Financial Reporting

An accurate, informative and timely accounting, management and financial reporting system is essential for the prudent operation of derivative activities. Internal auditors should determine whether the accounting and report preparations are being carried out by persons independent of the dealing function:

- a. Written accounting policies relating to trading and hedging with derivative instruments conform to the Generally Accepted Accounting Standards (GAAP);
- b. Accounting records accurately state the cost and market value of derivative transactions;
- c. Hedging transactions meet the criteria for exclusion from classification as trading transactions;
- d. Methods used to value derivative positions are appropriate and the assumptions underlying those methods reasonable;
- e. Revaluation procedures address the full range of trading instruments;
- f. Market rates used for revaluation are obtained independently;
- g. All off-market price transactions and off-premises dealings are properly accounted for and reported;

- h. Level of profit and risk positions are assessed based on earnings and risk; and
- i. Reward profile of specific products.

7.2.3 Legal and Regulatory Requirements

Internal auditors should review the relevant laws, regulations and guidelines particularly the Minimum Standards on Risk Management Practices for Derivatives issued by BNM and other relevant rules issued by the Securities Commission and Bursa Malaysia Exchange Berhad.

STUDENT PRACTICE 7

1. What is a derivative? (para 7)
2. What are the main risks associated with derivative products? (para 7.1)
3. Why is an independent research unit for derivatives important? (para 7.2.1(d))

8. INVESTMENTS IN DEBTS AND EQUITY SECURITIES

A financial institution's investment in debt and equity securities involves participation in the two main financial markets, namely, the capital market, and money and foreign exchange market. Invariably, investment in securities may account for a sizeable proportion of the financial institution's assets. As a result, inferior quality securities may have an adverse impact on its financial condition.

A typical investment portfolio usually comprises a combination of money market instruments, securities, public debt securities, equity securities (quoted and unquoted), equity-linked securities and Islamic private debt securities. Financial institutions usually maintain a trading portfolio and also an investment securities portfolio. Trading portfolio instruments are actively traded, while investment securities portfolio instruments are held as long-term investments.

8.1 Risks Associated with Investments

The risks are similar to those faced by credit and money market activities. Furthermore, although securities held in trading and investment portfolios share the same basic risk elements, the degree of significance of risks varies for each portfolio.

The primary risks inherent in the investment securities portfolio are related to the quality of assets held (i.e. credit risk), their marketability (i.e. liquidity risk) and interest rate fluctuations (i.e. interest rate risk). The risks are interrelated, e.g. an increase in market interest rates may affect other risk factors by decreasing marketability or by increasing the credit risk of the issuer's obligations. Another risk that investments in debt and equity securities are exposed to is country risk (if the debt or equity securities are raised by issuers outside the country).

In the trading portfolio, a higher volume of transactions makes settlement risk the primary risk. The counterparties' creditworthiness establish the degree of settlement risk.

Internal auditors should review the mechanism management uses to identify and manage risks associated with investment.

8.2 Internal Auditors' Role in Investment Risk Management

In order to mitigate the risks, financial institutions should establish a documented **sound investment policy** addressing the following:

- a. Objectives of the investment function;
- b. Permissible instruments;
- c. Portfolio composition;
- d. Personnel authorised to trade specific instruments;
- e. Parties with whom trade may be contracted;
- f. Trading limits/concentration limits/positions; and
- g. Geographic distribution limits.

This policy should be approved by the board of directors/management and be subject to periodic review vis-à-vis the investment portfolio.

a. Investment Strategy

The strategy should include investment objectives and goals, size of the investment portfolio, types and composition of securities, quality and maturity structure and target yields for the overall portfolio. It should also distinguish between securities held for investment and those for trading purposes. The investment strategy is to achieve profitable returns while simultaneously managing the risks within the investment portfolio. The strategy should commensurate with the risks the financial institution is prepared to assume.

Management should formulate policies and procedures for the purpose of analysing various investment alternatives. This is to meet the organisation's objectives after taking into consideration the level of management expertise, sophistication of the financial institution's control procedures and monitoring systems, its asset and liability structure and its capacity to maintain liquidity.

b. Policies and Procedures

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 investment strategy;
- c. Segregation of duties practiced for trading, processing, custody, payment and receipt, and maintenance of subsidiary records and accounting functions;
- d. No over-concentration of investment in a particular counter, sector or types;
- e. Trading and exposure limits imposed by the board are not breached;
- f. Payment is only made upon receipt of the confirmation of transfer of security, particularly 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 for unquoted shares or shares that are prescribed under the Central Depository System (scripless) are registered in the name of the nominee company;
- h. Revaluation exercise of the investment portfolio is carried out at least on a monthly basis;
- i. Adequate provision for permanent diminution in value has been made for securities of inferior quality; and
- j. Proper accounting of securities borrowed or lent out.

c. Accounting and Financial Reporting

Internal auditors should ensure that the classification of debt or equity securities, either for investment or dealing purposes, are in accordance with the GAAP. The classification of debt or equity securities, for either investment or dealing purposes, must comply with approved policies. Such a classification should be determined at the outset of the acquisition and any subsequent reclassification should be approved and properly documented.

Internal auditors should also evaluate the relevancy, accuracy, frequency and timeliness of reports submitted to the board and management. Such reports should cover all types of investments, gains or losses from disposals, provision for diminution in value and transfer of securities between investment and trading securities.

d. Legal and Regulatory Requirements

Financial institutions' investments should comply with the regulatory requirements issued by BNM and various regulatory bodies from time to time.

- i) Internal auditors should verify that the investment is within the limits for investment in private debt securities and for investments in shares.
- ii) Where a financial institution handles both its own as well as clients' investment portfolios, internal auditors should ensure that their institution observes the spirit of the BNM/GP7 (Guidelines on the Code of Conduct for Directors, Officers and Employees in the Banking Industry) on the code of ethics in the acquisition of various investments.

Where a financial institution is involved in bond trading for speculative purposes, there should be adequate policies and procedures in place to monitor its exposure. Among the limits that should be in place and monitored are position limits, cut-loss limits, exposure limits, dealer limits, etc. There should be a proper mechanism in place to promptly detect any breach in limits by dealers. Reporting to management on the financial institution's overall risk exposure in trading position should be made at regular intervals. Ratification of any breaches in limits should be timely reported to the relevant authority.

STUDENT PRACTICE 8

1. In which markets are debts and equity securities traded? (para 8)
2. What are the 3 major risks associated with investments (para 8.1)
3. What are the issues that a sound investment policy would address to mitigate risks associated with investments? (para 8.2)
4. Which BNM GP is important to observe non-conflict of interest between the financial institution's and its clients' investments? (para 8.2(d))

9. INFORMATION TECHNOLOGY

Information technology (IT) has become an integral part of banking and is considered the backbone of its operations. It has evolved from its role as merely generating and managing information and data, to a role where new products and services are not possible without strong IT involvement. In fact, IT is fundamental to support, sustain and enhance the growth of a financial institution.

Financial institutions expect that investment in information technology will deliver business value, and move from efficiency productivity gains towards value creation and business effectiveness. In view of its pivotal role and high costs of investment, there must be adequate safeguards to ensure the system is operationally reliable and secured against vulnerabilities. Operationally, confidentiality of information in the system must be safeguarded, integrity of information upheld and the system be fully secure. The risks of incorrect inputs and threats of the database being altered or insertion of unauthorised programs or viruses as well as hackers can undermine the reliability of information.

9.1 Risks Inherent in Information Systems

The main risks confronting IT, as illustrated in the "Guidelines on Management of IT Environment (GPSIS 1)" issued by Bank Negara Malaysia, are stated below. These are some of the main risks and the list is not exhaustive.

a) Strategic Risk

The risk to financial businesses arising from adverse business decisions or improper implementation of the decisions on IT that will result in loss of competitive advantage, further significant incurrence of capital outlay on IT and incapability of the system in meeting organisational needs.

b) Compliance Risk

The risk to financial businesses arising from non-conformance with or violations of laws, statutory requirements or ethical standards through the use of IT that will result in financial losses and legal/regulatory problems.

c) Operational Risk

The risk to financial businesses arising from system failures caused by system breakdowns, system disruptions and interruptions that will impede business operational functions.

d) System Security Risk

The risk to financial businesses arising from the lack of or absence of system security, either by the computer hardware or software, or weak implementation of security measures that will result in the system being compromised, fraud, malicious damage to data and program or error.

e) System Support Risk

The risk to financial businesses arising from the lack of or absence of system support, either by the computer hardware or software vendor, service provider and outsourcer or the system itself that will result in the failure of or interruptions to the operations of the information system.

f) Business Resumption Risk

The risk to financial businesses arising from system non-recoverability and continuity that would result in financial losses.

g) Reputation Risk

The risk to financial businesses arising from negative public opinion through the use of IT that will result in financial and non-financial losses, such as loss of public confidence.

9.2 Internal Auditors' Role in the Risk Management of Information Technology

Information technology (IT) refers to an environment where a computer of any type or size is used to process information that is of significance to management decision-making.

Specifically, IT auditors should review:

- a. the effectiveness of IT in supporting the financial institution's business activities and the adequacy of controls over the IT management;
- b. the systems development and programming; and
- c. the computer operations and security, teleprocessing, and data integrity.

The IT audit also includes the BNM guidelines on minimum IT audit coverage for the electronic funds transfer (EFT) system and credit card operations.

9.2.1 Board and Management Oversight

For proper IT governance, the board of directors is responsible to ensure adequate steps, measures and procedures are in place to comply with the GPSIS 1 Guidelines. Similarly, senior management oversight should be established in governing the day-to-day IT activities. There should also be an IT Steering

Committee whose main duties include overseeing the development and maintenance of the IT strategic plan.

Internal auditors should establish that there is proper and organised structure in place to oversee the overall IT function in a financial institution. The board of directors and senior management are aware of and understand their responsibilities in ensuring implementation of good IT governance, and the risks and constraints of IT in order to provide effective strategic directions to the institution.

IT auditors should pay particular attention to the following:

- a. Proper structure and organisation in overseeing the IT functions, at the respective levels:
 - i) Board of directors,
 - ii) Senior management, and
 - iii) IT Steering Committee.
- b. A well conceived IT strategic plan is in place that reflects the business strategy and matches the IT needs for a defined future period;
- c. The IT department's organisational structure provides for a proper reporting line. Segregation of incompatible functions within IT processing activities is practiced, i.e. system development and programming, computer operations and security implementation. Nevertheless, in cases where such segregation may not be possible – normally found in small IT installations – IT auditors should determine the adequacy of compensating controls;
- d. There are proper policies and procedures stated to adequately provide the basis for establishing and maintaining proper IT management to prevent or reduce internal and external threats;
- e. Adequate and availability of manpower and staff who are adequately trained and competent;
- f. Business resumption and contingency plans are in place and adequate
- g. Proper project management and monitoring are in place, with focus on adequacy of operational controls; and
- h. Internal audit is given the right to access and communicate with any member of staff and to examine any activity or entity of an institution.

9.2.2 System Security

System security failures can be very costly and disruptive to an institution's business. Minimum standards should be implemented to ensure that logical access controls are one of the primary safeguards. In addition, there should be a well documented and designed policy, procedures and awareness programmes. Authentication management and password controls are other key areas. These in turn must be supported by proper log-in controls, logical access, activity monitoring, data and database controls and application controls.

In assessing the adequacy of computer security, IT auditors need to ensure the following:

- a. There is a proper security policy communicated to users;
- b. Adequate authentication management and tools are in place and operating as laid down;
- c. The security administration function is clearly and properly assigned to competent staff;
- d. Procedures on security administration, password issuance and maintenance, and follow-up on access violations, are adequate and effective;
- e. Assignment of access capabilities to users is properly done and in accordance with the access rule. Access to data and program altering utilities, system parameters, log and password files should be restricted. If a database management system is used, the assignment of access to the database should also be reviewed to ensure proper assignment of capabilities;
- f. Logging, reporting and reviewing of activities, especially abnormal activities are adequate and effective; and
- g. There is a policy on use of cryptographic controls for protection of critical/sensitive information.

9.2.3 Systems Development and Programming

There should be minimum standards in place to ensure that system development activities are sufficiently controlled to ascertain the integrity of data and system. Poor management and controls over system development could result in the following:

- Inadequate specifications,
- System design error,
- Lack of controls in programme change management,
- System not adequately tested,
- Incomplete and inadequate documentation, and
- Frequent data and system integrity problems.

The IT auditors' role in the systems development and programming functions should not only be limited to auditing of systems already implemented. They should also participate, in a consultative/advisory capacity, in the development of new IT systems to ensure that appropriate audit and control procedures are designed and built into the systems. While participating in the systems development process, IT auditors should maintain their objectivity and independence and avoid participating in any operational responsibility for the system.

The IT auditors' main areas of concern should include the following:

- a. An effective project management system is employed to monitor and control application development projects;
- b. Standards and procedures on the systems development and programming function are available and comprehensive;
- c. The development of application systems has complied with standards for the systems development and programming function;
- d. Segregation of incompatible functions, e.g. application programmers should not have "write" access to production data and not be involved in the maintenance of operating systems. System programmers should not have access to production data and not be involved in the maintenance of application programmes;
- e. The production system is properly segregated from the development or testing system;
- f. Documentation maintained on the application systems should be comprehensive and current. Documentation should at least include user manuals, computer operator instructions, flowcharts and descriptions of the application systems and programs;
- g. Controls over the maintenance of application programs and operating systems are adequate and effective to ensure data and programs integrity in the system. Procedures should ensure that all requests for changes are authorised and attended to timely. Only authorised programs are catalogued to the production system and the relevant documentation updated to reflect the changes. Controls over urgent requests for changes to application programs or operating systems should also be in place since such requests will normally bypass the need for prior written authorisation;
- h. There must be sufficient testing under different conditions/volume to ensure that the design and overall reliability are in accordance with the original specifications;
- i. Test plans and results are adequately maintained for review;
- j. A secured library for programs pending migration to the production environment should be established;
- k. Controls of source codes into object codes should be adequate;
- l. Controls over usage of powerful utilities with data altering capabilities are adequate and effective; and
- m. Post implementation reviews are conducted to assess the application's operational performance.

9.2.4 Computer Operations

Computer operations activity involves the operation and maintenance of computer and telecommunications equipment. Adequate operating standards are necessary to ensure that the information produced by the computer system is accurate, reliable and safeguarded against errors, fraudulent manipulation and accidental destruction of records.

Accordingly, there must be proper standards and procedures covering computer operation functions, complemented by proper maintenance of the computer centre. There should be in place a system of monitoring of operational activities and a set of emergency procedures.

IT auditors should pay particular attention to the following areas:

- a. Computer operations procedures are adequate and complied with;
- b. Adequate maintenance of the computer centre, ensuring the centre and surrounding areas are clean, neat and orderly to reduce the possibility of fire and damage to the computer and telecommunications equipment;
- c. Physical controls, including controls to prevent unauthorised entry to the computer centre and equipment are adequate and effective. Such controls may include 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 other disasters;
- d. Controls are adequate to ensure correct tapes, disks or other storage media are used and data files are correctly written or read;
- e. Procedures are in place for segregation of incompatible duties in the computer operations environment;
- f. Adequate detective and preventive controls are in place; and
- g. Procedures for the disaster recovery plan comply with BNM guidelines.

9.2.5 Communications Network

Communications convey information and provide a channel of access to information systems. A breach in the integrity of the network can be extremely costly and is a reputational risk.

IT auditors should review the following areas:

- a. Adequate procedures are in place which include measures to restrict access to files, transactions and terminals, logging, reporting and reviewing of deviations from normal transactions and backup procedures;
- b. Network designs conform with sound principles and are dynamic enough to cope with anticipated changes;
- c. The security system implemented to protect data transmitted over the telecommunication media is adequate;
- d. All transmissions received are from authorised terminals and users. There should be an effective filtering device in place;
- e. Procedures on error detection and recovery are adequate and effective;
- f. Network activities are logged, reported and reviewed by the network supervisor; and
- g. Procedures are adequate to ensure system reliability.

9.2.6 Data Integrity

Most financial institutions have installed computerised application systems to process their operational activities. Specific application reviews should be conducted by IT auditors to test data integrity and reliability in a specific application system. Computer-Assisted Audit Techniques (CAATs) should be used to improve checking of data integrity by auditing “through” the computer system.

The following areas should be reviewed:

- a. Controls over input of data are adequate and effective to ensure accuracy and completeness of data and to prevent initiation of transactions by unauthorised personnel;
- b. Programmed controls, e.g. edit checks and reasonable checks, are adequate to ensure processing of information is done correctly. Such controls should include procedures on handling rejected and resubmitted data; and
- c. Controls over output distribution are adequate. Exception reports should be provided to authorised personnel for verification and error correction purposes.

9.2.7 Electronic Funds Transfer System

There are two types of electronic funds transfer (EFT) systems:

- a. A wholesale EFT system which includes RENTAS and SWIFT, and
- b. Automated teller machines (ATMs), point-of-sale (POS) system and debit cards.

Management is responsible for establishing policies and procedures for the EFT system that provides guidelines on the approving authority and discretionary powers, organisation of records and files, internal supervision in identifying irregularities and the relevant follow-up or punitive actions to be taken.

In reviewing the wholesale EFT system, IT auditors should focus on:

- a. Internal policies and procedures on funds transfer activities are adequate and complied with;
- b. Adequate controls over origination of input documents, processing and output distribution;
- c. Adequate teleprocessing controls to ensure confidentiality, integrity and availability of data transmitted over the system;
- d. Segregation of incompatible functions is enforced; security administration, data entry and transmission functions should be segregated.
- e. Sensitive items, e.g. master passwords and log-in IDs, are kept under dual custody;
- f. Reconciliation of the number of messages and value of funds transmitted is performed on a timely basis to minimise exposure to erroneous or unauthorised transfers of funds;

- g. Adequate reports are printed to monitor activities in the RENTAS/SWIFT system; and
- h. Adequate physical security for the RENTAS/SWIFT terminals, source documents and system-generated reports.

In reviewing the retail EFT system, IT auditors should focus on the following:

- a. Procedures on ATM operations are available and adequate;
- b. Adequate controls over procurement, processing, storage and distribution of plastic cards and PIN mailers;
- c. PINS are encrypted on all files and databases and during transmission;
- d. Sensitive items (e.g. PIN keys used during PIN generation and verification, and documentation on encryption, decryption and PIN-generation processes) are securely kept;
- e. Segregation of incompatible functions is practised. Card processing and custodianship should be segregated from PIN processing and custodianship;
- f. PIN generation should be segregated from PIN processing and custodianship;
- g. User IDs and passwords to access the system have been assigned to authorised personnel;
- h. Controls over origination of input documents, processing and output distribution are adequate;
- i. Procedures on the PIN-generation processes are adequate including the immediate deletion after use of any recording media in the process of assigning, distributing, calculating or encrypting PINs;
- j. The financial institution has complied with the applicable laws and BNM guidelines; and
- k. For a shared ATM network:
 - Adequate audit trails are maintained for all transactions;
 - Rejected items are properly reported and accounted for; and
 - Procedures on balancing and settling transactions are adequate.

9.2.8 Credit Card Operations

The 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 risks inherent in credit card operations is credit risk. Financial institutions face the risk that customers may not be able to repay the outstanding balance in their credit card bills. Hence, financial institutions should have an internal credit assessment policy for purposes of conducting a proper credit scoring exercise in approving or declining credit card applications, and in determining the appropriate credit limit for each approved applicant. Management is responsible for establishing policies and procedures that should provide guidelines on credit appraisal, approving limits, card processing and supervision, merchant recruitment and termination, MIS and record keeping for this facility.

The IT auditor's minimum audit coverage in the review of credit card operations is as follows:

- a. Policies and procedures governing credit card operations are adequate and complied with;
- b. Incompatible functions within credit card operations are segregated; card processing functions such as card approval, transaction authorisation, accounting, card embossing and card distribution should be segregated;
- c. No credit limits in excess of the approving officers' authority are given to approved credit card applications;
- d. Adequate procedures on input, processing and output of credit card applications and transactions to ensure accuracy, completeness and validity of data entered into the credit card application system;
- e. Adequate and effective procedures on the assignment and maintenance of user IDs and passwords for the credit card application system;
- f. Adequate controls over maintenance of account status, e.g. deactivation of cards reported lost/stolen;
- g. Controls over the procurement, embossing and encoding, storage and distribution of credit cards are adequate;
- h. Adequate procedures on the PIN generation process, e.g. the immediate deletion after use of any recording media in the process of assigning, distributing, calculating or encrypting PINs (ATM system);
- i. Management information systems are adequate, e.g. reports on accounts in excess of limits, accounts with arrears, non-performing loans, accounts with disputes, daily excess authorisation reports and fraud cases;
- j. The financial institution has complied with the applicable laws as well as BNM directives and guidelines; and
- k. Fraudulent transactions and chargeback losses.

STUDENT PRACTICE 9

1. What is system security risk and its impact to a financial institution? (para 9.1(d))
2. For IT governance, which groups of personnel and their responsibilities in a financial institution should the internal auditors review?. (para 9.2.1(a))
3. What are some of the impact of poor management and controls over system development? (para 9.2.2)

10. OTHER OPERATIONAL AREAS: HEAD OFFICE OPERATIONS

Head Office sets the direction and provides the leadership for the financial institution not only in the area of business strategies but in the area of corporate governance as well. Therefore, it is of importance that Head Office operations must be properly run so as to set the tone from the top that effective and high standards of corporate governance practices are being adopted and undertaken. Amongst the areas/functions that can be covered under Head Office operations are human resources, accounting systems, property procurement/management, etc.

10.1 Internal Auditors' Role in Risk Management of Head Office Operations

Briefly, the scope of an audit on human resources is as follows:

- a. Adequacy of existing human resource policies for recruitment, manpower planning, compensation and benefits, training and disciplinary actions;
- b. The above polices are implemented with proper guidelines or documented procedures;
- c. Compliance with the relevant regulatory requirements pertaining to payroll, such as the Income Tax Act, particularly on scheduled tax deductions, EPF and SOCSO reductions, etc.
- d. Accounting and payroll controls to ensure that salaries and allowances are only paid to rightful staff, and
- e. Ensuring that personnel records are up-to-date in terms of salaries, bonuses, increments, benefits granted and educational levels.

The audit scope for the accounting system is as follows:

- a. Adequacy of accounting policies and procedures, including those pertaining to loan provisioning, fixed assets, income recognition, Islamic banking practices, etc;
- b. Accounting manuals and consistency in accounting practices;
- c. Institution of proper accounting automation packages in ensuring sound accounting and administrative controls in generating accounting records;
- d. Accuracy and completeness of financial reporting which is consistent with the requirements stipulated under the BNM/GP8 guidelines and those of the Malaysian Accounting Standards Board; and
- e. Reconciliation of nostro and vostro accounts.

The audit scope for property procurement/management involves the following:

- a. The identification of the financial institution's properties and assets;
- b. Observation of purchasing procedure in accordance with prescribed policies and practices;
- c. Adoption of a standard depreciation policy in accordance to accounting standards;
- d. Adherence to write-off procedures and asset disposal guidelines;
- e. Adequate upkeep and maintenance procedures, which may include outsourcing of work to other third parties;

- f. Tendering policies and procedures; and
- g. Payment of rates, e.g. quit rent, assessment, insurance and utilities.

11. OTHER OPERATIONAL AREAS: INSURANCE UNDERWRITING AND CLAIMS

11.1 Insurance Underwriting

Insurance underwriting is the process by which an insurance company assesses and accepts risks, or liabilities, under the terms of an insurance policy (contract) for a sum of premium, guaranteeing payment in the event of loss or damage.

All insurance contracts indemnify the insured for losses that may arise under a policy. Thus, the insured is reimbursed for the actual loss under the terms of the policy, and not allowed to profit from the loss.

Two exceptions to the indemnity rule are life assurance and personal accident policies. Under these policies, in consideration for a sum of premium, the full sum assured becomes payable upon the death of an assured, or for loss of limbs at a predetermined sum under a personal accident policy. Presumably, the indemnity rule cannot be applied to life (and personal accident) as it is difficult to value a person's life.

For prudence, an insurance company only retains part of the risk it has accepted and transfers the remaining portion to other insurers or treaty partners. This cession of risk is done through the following arrangements:

a. Treaty Reinsurance

Long-term arrangements (reviewed periodically) with treaty reinsurers on pre-determined terms whereby risks exceeding an insurance company's retention limit are automatically ceded to the treaty partners.

b. Facultative Reinsurance

Facultative reinsurance arrangements (with other insurance companies) which are made separately for each risk prior to acceptance of risks that exceed treaty limits.

c. Cession to Malaysian National Reinsurance Berhad

Cession to Malaysian National Reinsurance Berhad (MNRB) in accordance with 'voluntary' cession arrangements.

Examples of the main categories and types of insurance coverage are listed in Appendices I and II of this chapter.

11.2 Risk Assessment and Management

An insurance company's principal activity is the underwriting of risks. Therefore, when developing the underwriting strategy, management should put in place a mechanism to identify and manage risks associated with prudent underwriting.

Hence, it is essential for management to have in place the board's approved sound underwriting policies, procedures and a well-established system of internal control. Internal auditors play an important role to ensure adherence to policies, procedures and the internal control system.

The risks associated with insurance underwriting and internal auditors' roles are discussed below.

11.2.1 Strategic Risk

a. Portfolio Mix

The mix of the various classes of risk accepted is well balanced and in the proportion pre-determined by management. There should not be over-exposure to any particular class of risk.

b. Level of Risk Retention

Management should fix the retention level for the various types and classes of products for general insurance and per life assured basis for life insurance after taking into account the company's shareholder funds, its profitability and risk tolerance.

c. Treaty Arrangement

Treaty partners should not only be of good financial standing but should also have the capacity to accept large risk exposures so as to allow the insurance company sufficient leverage to bid for large risks and be a significant player in the insurance industry. The audit should encompass whether there have been reviews of the treaty partners' financial statements and whether treaty arrangements are subject to annual review.

d. Risk Accumulation

A system is in place to identify accumulation of risks (general) and multiple policies (life) for checking by underwriters before risk acceptance. This ensures that risks are spread out and a single event does not severely affect an insurance company's bottom line.

e. Authority Limits

The underwriting authority limits for risk acceptance should commensurate with the underwriting abilities and competence of the assigned staff. This is important to ensure that only quality risks as per the company's guidelines are accepted and undesirable risks are either weeded out or subject to more stringent underwriting requirements.

f. Feedback on Claims Statistics

A system should be in place to speedily communicate feedback on claims statistics and large claims to the underwriting department. This is important as underwriting policies can be reviewed and reformulated, the target portfolio mix changed and renewals of large unprofitable risks avoided.

11.2.2 Credit or Counterparty Risk**a. Reinsurers**

Treaty reinsurers should be properly approved and of good security. There should be an established system for vetting the quality of reinsurers, periodically reviewing their financial standing and setting limits of exposure to any one reinsurer.

Similar systems should also be in place for facultative reinsurers with limits of exposure and categorisation according to financial standing.

For reinsurance placements made through brokers, they should be of reputable standing and required to promptly submit placement slips, signed reinsurance policies or treaty documents to the company.

b. Co-insurers

Since co-insurers share large risks with the insurance company, their credit-worthiness should be established before participation to ensure there will be no settlement problems in premium collection and claims recovery.

c. Intermediaries (Agents, Consultants, Brokers, etc)

Procedures are instituted for the appointment and conduct of intermediaries, in particular, monitoring of errant intermediaries, such as agents, consultants, brokers and adjusters. This will minimise possibilities of further credit exposures and of intermediaries giving false representation on policy benefits, terms and exclusions. The cover note control system should be strictly enforced to limit losses from errant agents.

d. Direct Clients

Direct clients should be closely monitored for premium collection especially for policies exceeding the credit period. Policies of errant clients should be cancelled to reduce exposure once it becomes clear that premium settlement is not forthcoming. Internal auditors should also assess whether there are proper mechanisms in place to ensure that premiums are paid and collected within the time frame as stipulated by BNM, i.e. 30 days for motor insurance and 60 days for non-motor cases, and with a premium warranty clause.

11.2.3 Documentation Risk

a. Policy Documents

Policy documents should be explicitly worded and clear on the terms of the insurance coverage. Policy exclusions should also be clearly worded to avoid disputes in the event of claims.

b. Treaty Documentation

All treaty reinsurance arrangement terms should be supported by adequately vetted legal documentation.

c. Facultative Reinsurance Confirmation

Reinsurers confirm all facultative reinsurance placements by telex/fax before risk commencement and follow up with closing slips.

d. Agency Documentation

All agency (life and general) appointments are supported by adequately vetted legal documentation.

11.2.4 Regulatory Risk

- a. **Premium rates** for life business are charged in accordance with the rates approved by a qualified actuary, whilst for the tariff-rated class of general insurance business, premiums charged are in accordance with the tariff.
- b. A **register of policy** is maintained as prescribed by the Insurance Act 1996 and the Takaful Act 1984.
- c. Only **registered agents** are allowed to transact insurance business on the company's behalf.
- d. **Commissions** (inclusive of agency related expenses and other benefits) paid to intermediaries are in accordance with the limits stipulated in BNM's Operating Cost Control (OCC) Guidelines.
- e. The company's **management expenses** do not exceed the limits stipulated in the OCC Guidelines.
- f. Payment and remittance of motor premiums comply with cash-before-cover (CBC) insurance regulations.
- g. **Payment of premiums** to insurance companies within 60 days of commencement of risk (for most classes of general insurance business) is in compliance with the premium warranty clause.
- h. **Local retention** is optimised and fronting arrangements with foreign insurers avoided.
- i. Management review and supervision are in place to **ensure accuracy of data and information** reported in the returns submitted to BNM.

- j. **Bond underwriting** is in accordance with the Persatuan Insuran Am Malaysia's (PIAM) guidelines particularly on premium collection and collateral submission prior to release of the bond guarantee document.

11.2.5 Investment Risk

a. Risks Inherent in Investment

The risks inherent in investment include credit, price, liquidity, operational and country risks. The level of the risks inherent in investment depends on whether it is held for long-term or short-term investment and the complexity of the investment products. Internal auditors should review the mechanism management uses to identify and manage these risks.

b. Investment Strategy

i) Board approved investment strategy

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

ii) Management formulated investment policies and procedures

Management should formulate policies and procedures for the purpose of analysing various investment alternatives. This is to meet the financial institution'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.

11.2.6 Internal Auditors' Role in Risk Management of Insurance Investments

Internal auditors should, therefore, focus on the following significant areas:

- Adequacy of and compliance with policies and procedures;
- Investment operations are in line with investment strategy;
- Segregation of duties for trading, processing, custody, payment and receipt, and maintenance of subsidiary records and accounting functions is practised;
- No over-concentration of investment in a particular counter, sector or type;
- Trading and exposure limits imposed by the board are not breached;

- Payment is only made upon receipt of confirmation of transfer of security, particularly in the case of scripless negotiable instruments of deposits or instruments that are normally entrusted with a central or an authorised depository;
- Share certificates or shares that are prescribed under the Central Depository System are registered in the name of the nominee company; and
- A revaluation exercise is carried out on the investment portfolio at least on a monthly basis, and adequate provision has been made for permanent diminution in value for securities of inferior quality.

11.2.7 Operational or Internal Processes Risk

a. Underwriting Approval

The Underwriting Worksheets, Approval Slips and Cover Notes have been properly approved to ensure only risks as per underwriting guidelines are accepted and that declined or hazardous risks are rejected. Referred risks accepted should be specifically approved and on an accommodation basis or with premium loadings.

b. Prior Facultative Reinsurance Confirmation

Prior confirmation of facultative reinsurers is obtained before acceptance of large risks exceeding treaty capacity for both new and renewal risks.

c. Risk Surveys for Large Risks

Risk surveys (supported by survey reports) are done for risks exceeding a certain sum to ensure that all physical hazards are identified and steps taken to improve the risks before acceptance. Otherwise, the risk should be declined if too hazardous.

d. Declaration in Proposal Forms

Proposal forms are properly completed and signed and all relevant information declared by the insured. This will ensure that moral hazards are mitigated as claims arising due to misrepresentation of material facts by the insured can be rejected.

e. Submission of Financial Statements

Where appropriate, the insured's financial statements should be obtained for perusal to ensure the insured is not suffering heavy losses that can be a moral hazard for an insurance company.

f. Monitoring of Renewal Business

Renewal business should be closely monitored whereby steps should be taken to renew profitable risks while unprofitable risks should not be invited for renewal.

g. Cover Note Control Procedures

Cover note control procedures and system controls encompassing requisitioning, issues to agents and subsequent retrieval from agents should be strictly adhered to and unreturned cover notes speedily reported as exceptions.

h. Processing of Risks Accepted

There should be a proper system in place to ensure all risks accepted from co-insurers, brokers, other insurers (i.e. inward risks) and agents are processed into policies for prompt recognition of premium.

11.3 Insurance Claims**Board's Approval Needed for Management-formulated Claim Policies and Procedures**

Management is responsible for establishing proper and sound policies and procedures pertaining to the administration of claims portfolio. These policies and procedures may be in the form of guidelines or a claims manual. The policies on claims, which should be approved by the board, generally cover approved limits for competent personnel and the claims committee, prompt and fair settlement of claims, reporting of large losses, payment 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 sale or disposal of wrecks, basis of determining reserves for outstanding claims including Incurred But Not Reported (IBNR) and processing and disbursement of claims. The claims procedures should include feedback on claim statistics to the Underwriting Department for review of underwriting policies.

11.3.1 Internal Auditors' Role in Areas of Insurance Claims

Internal auditors should address the following areas of audit concern as extracted from BNM/GP10 Part V:

- i) Adequacy of policies and procedures;
- ii) Claims process complies with approved policies and procedures;
- iii) Segregation of duties and responsibilities relating to claims processing, approval and payment is practised;
- iv) Register of claims is maintained as prescribed by the Insurance Act 1996 and the Takaful Act 1984. All claims or known losses should be promptly registered with reasonable provision (even in cases where limited information is available);
- v) Claims data are accurately recorded;
- vi) Proper and fair claims settlement practices have been adopted –
 - Prompt in processing and paying claims with no “delay tactics”;
 - Disbursement of claims are properly approved and supported by appropriate documentation;

- Preventive measures are in place to deter fraud; and
 - Requirements stipulated in guidelines issued by the Jabatan Pengawalan Insurans, BNM on claims settlement practices and guidelines to combat motor insurance fraud (general business) are complied with.
- vii) Estimates of preliminary loss reserves are reasonable, regularly reviewed and updated upon receipt of fresh and relevant information. Reserves on every outstanding claim should be reviewed at least once a year by experienced and competent officers;
- viii) Claims settled through compromise or on an ex-gratia basis are reasonable, justifiable and not subject to abuse;
- ix) All recoveries in respect of salvage, subrogation or from (treaty and facultative) reinsurers are properly recorded and collected on a timely basis. In cases involving motor claims, adequate controls are instituted over the sale of wrecks;
- x) Outstanding loss reserves, inclusive of IBNR, are adequate at any point of time and are as per the BNM/GPI 12 guidelines. For this purpose, the IBNR established at the last balance sheet date would be regarded as the IBNR required at any point of time until the next balance sheet date;
- xi) A proper monitoring system is in place to record accumulation of claims arising from a particular event or within a particular period for purposes of reporting to Excess of Loss (XOL) reinsurers and for review of adequacy of XOL cover; and
- xii) A system is in place to identify maturing life policies to enable payments to be made promptly.

In addition, internal auditors should also be mindful of the Guidelines on Claims Settlement Practices (JPI/GPI 14) dated 16 September 2003 stating, among others, the minimum duration for processing of claims.

STUDENT PRACTICE 10

1. How does an insurance company cede its risks? (para 11.1)
2. How does portfolio mix and risk retention limits mitigate strategic risk in insurance underwriting? (para 11.2.1(a)&(b))
3. What are the areas internal auditors should focus on to manage operational risk in insurance underwriting? (para 11.2.6)
4. List any five areas of audit concern when dealing with insurance claims. (para 11.3)
5. What is bond insurance? (Appendix I)
6. What is basic term assurance under life assurance coverage? (Appendix II)

12. OTHER OPERATIONAL AREAS: BUSINESS CONTINUITY MANAGEMENT

Business continuity management (BCM) entails enterprise-wide planning and arrangement of key resources and procedures that enable the institution to respond and continue to operate critical business functions across a broad spectrum of interruptions to the business, arising from internal or external events. The BNM Guidelines on Business Continuity aim to ensure that financial institutions:

- have in place a comprehensive BCM framework, which includes a business continuity policy,
- establish a comprehensive BCM programme to formulate, implement and test the business continuity plan (BCP) and disaster recovery plan (DRP),
- review and update the BCP and DRP continuously to reflect changes in the operating environment, and
- provide sufficient information to the board of directors to enable them to discharge their responsibilities under the Guidelines.

BCM encompasses disaster recovery for IT systems, crisis management and contingency planning. Hence, the financial institution is required to ensure that internal linkages with crisis management and emergency response procedures as well as external dependencies on key service providers/vendors are adequately considered during business continuity planning. Safeguard measures should also be undertaken on human life and business assets / premises.

The BCM life cycle comprises the following:

- a. analysing the financial institution's business functions and their criticality through risk assessment and business impact analysis,
- b. formulating appropriate and workable BCM recovery strategies based on the risk assessment and business impact analysis,
- c. developing and implementing BCP and DRP,
- d. Testing the plans,
- e. Reviewing and maintaining the plans,
- f. Auditing the plans, and
- g. Conducting ongoing awareness programmes and communication, training and education on BCM.

12.1 Internal Auditors' Role in Business Continuity Management

Internal auditors should be aware of the requirements stated in the Guidelines on Business Continuity Management (BCM) issued by Bank Negara Malaysia.

The broad issues the internal auditors need to address relating to BCM are that the institution:

- a. Has in place a comprehensive BCM framework which includes a business continuity plan (BCP);
- b. Establishes a BCM Committee and a working committee, with a comprehensive BCM programme to formulate, implement and test the business continuity plan ;
- c. Reviews and updates the business continuity plan and disaster recovery plan continuously to reflect changes in the operating environment; and
- d. Provides sufficient information to the board of directors to enable it to discharge its responsibilities under the Guidelines.

Internal auditors should note the following principles:

- i. There is board and management oversight on the implementation of an effective BCM. In this respect, there must be a BCM Committee and clearly defined policies as well as a clear definition of roles and reporting lines of individuals/committees responsible for BCM;
- ii. There should be a structured risk assessment process to identify potential threats and risk assessments should be performed on a regular basis, at least annually;
- iii. A business impact analysis is also undertaken regularly to identify areas of greatest impact as a basis to draw up the BCP;
- iv. Critical business functions essential for the development of recovery strategy are identified, and an appropriate strategy for recovery developed accordingly;
- v. For all critical business functions identified, there should be an established maximum tolerable downtime (MTD) and recovery time objective (RTO). The goal is to develop a BCP that details the procedures and minimum level of resources required for recovery.
- vi. There should also be identification of the minimum services and recovery strategy should be tailored to the different level of disruptions;
- vii. There must be a formal business continuity plan and disaster recovery plan formulated and approved by management that is effectively implemented and properly maintained by all units. Internal auditors must review on annual basis the financial institution's level of commitment to BCM and overall preparedness;
- viii. Alternative and recovery sites should be identified and in a state of preparedness for usage in event of any major disruption. Similarly, systems and critical business information records must be available for recovery in the event of major disruption;

- xi. The BCP and DRP must be reviewed and tested regularly to ascertain their functionality and effectiveness. Internal auditors must be involved in major functional BCP and DRP testings with an independent assessment report being given to the Audit Committee. An audit report on BCM and BCP testings is submitted to BNM not exceeding 2 months after its tabling at the Audit Committee together with comments (from the Audit Committee);
- ix. The BCP should incorporate the strategy and approach for communication with relevant internal and external stakeholders; and
- x. In the event certain functions are outsourced, the institution should ensure that the risk arising from outsourcing does not affect its business continuity preparedness. Internal auditors should ensure and review that BCP testing is undertaken by the outsourcing vendor. An audit report is to be prepared and submitted to the Audit Committee

13. OTHER OPERATIONAL AREAS: ISLAMIC BANKING – THE SHARIAH COMMITTEE

Compliance with the Shariah principles is an integral part of Islamic banking. As such, there is a need for a comprehensive and effective *shariah* framework to harmonise Shariah interpretations and strengthen the regulatory and supervisory oversight of Islamic banking. Towards this, Bank Negara Malaysia has prepared the Guidelines on the Governance of Shariah Committee for the Islamic Financial Institutions (BNM/GPS 1), which seeks to regulate the governance of the Shariah Committee of an Islamic institution.

The objectives of the Guidelines are:

- a. To set out rules, regulations and procedures in the establishment of a Shariah Committee;
- b. To define the role, scope of duties and responsibilities of a Shariah Committee; and
- c. To define the relationship and working arrangement between a Shariah Committee and the Shariah Advisory Council of Bank Negara Malaysia.

Essentially, the broad guidelines are as follows;

- a. Every Islamic financial institution is required to establish a Shariah Committee;
- b. The Shariah Committee shall report to the board of directors of the Islamic financial institution;
- c. A member of the Shariah Committee shall at least have qualification or possess necessary knowledge, expertise or experience in:
 - i. Islamic jurisprudence (*Usul al-Fiqh*), and
 - ii. Islamic transaction/commercial law (*Fiqh al-Mu'amalat*).
- d. Composition of the Shariah Committee shall be a minimum of three; and
- e. A person can act as member of a Shariah committee in one institution of the same nature;

-
- f. The duties and responsibilities of the Shariah Committee are:
- i. To advise the Board on Shariah matters in business operations, ensuring compliance with Shariah principles at all times;
 - ii. To endorse Shariah Compliance manuals, which shall state the conduct of the Shariah committee's meetings and manner of compliance with any Shariah decision;
 - iii. To endorse and validate relevant documentations, such as terms and conditions in the proposal form, contract, agreement and other legal documentation, and product manual, sales illustrations and other;
 - iv. To assist related parties, such as auditors, legal counsel or consultants on Shariah matters for advice upon request;
 - v. To advise on matters referred to the SAC;
 - vi. To provide written Shariah opinions, particularly where the Islamic institution make reference to the SAC for advice or where the Islamic institution submits an application to Bank Negara Malaysia for new product approval; and
 - vii. To assist SAC on reference for advice.
- g. The duties and responsibilities of Islamic financial institutions are:
- i. To refer all Shariah issues to the Shariah Committee for advice and decision;
 - ii. To adopt and take the measures necessary based on the Shariah Committee's advice;
 - iii. To ensure that product documents be validated by the Shariah Committee;
 - iv. To have a Shariah Compliance manual;
 - v. To provide access to relevant documents, transactions, manuals and other relevant information for them to discharge their duties effectively;
 - vi. To provide sufficient resources, such as budget allocation, independent expert consultation, training etc;
 - vii. To remunerate the members of the Shariah Committee accordingly, reflective of their roles and functions.

13.1 Internal Auditors' Role on Shariah Audit

The internal auditor's role in auditing Islamic banking will not differ very much from auditing conventional banking in terms of business performance, operations, risk management and controls. What is required more of the auditor is an understanding and preferably, technical knowledge of Islamic commercial contracts to conduct a Shariah compliance audit. Briefly, the Shariah compliance audit would entail the auditors to check that:

- i. There are no violation of Shariah principles in the contract and related correspondence;
- ii. Proper procedures and practices are in place for each Islamic contract;
- iii. Supporting documents are complete and properly kept; and
- iv. Processing controls in place in the system to support the contracts and produce correct information.

Further details on Shariah compliance audit are given in Section 7, Chapter 3 of this manual.

14. OTHER OPERATIONAL AREAS: BASEL CAPITAL ACCORD II

The Basel Capital Accord defines a standard methodology for calculating the capital to assets ratio. Basel II is the second of the [Basel Accords](#) and is more than just a definition of the capital to assets ratio. The purpose of Basel II, which was initially published in June 2004, is to create an international standard that banking regulators can use when creating regulations about how much capital banks need to put aside to guard against the types of financial and operational risks banks face. Basel II attempts to accomplish this by setting up rigorous risk and capital management requirements designed to ensure that a bank holds capital reserves appropriate to the risk the bank exposes itself to through its lending and investment practices. Essentially, this translates to mean the amount of capital the bank needs to hold to safeguard its solvency and overall economic stability has to be in tandem with the bank's exposure risk. Details on Basel II Accord are documented in Chapter 4.

14.1 Internal Auditors' Role in Compliance with the Basel II Accord

The Basel II Accord recommendations will be the basis of computation of the Risk Weighted Capital Ratio (RWCR). Accordingly, internal auditors should:

- i. Review and validate that the assumptions used in any of the risks models adopted are reasonable and applied consistently;
- ii. Ensure data used for generation and computation is reasonable and based on the institution's historical database and experience;
- iii. Computation is fairly accurate and consistent with the policies/methodology adopted; and
- iv. Compliance issues relating to Basel II are being adhered to.

15. OUTSOURCING

Bank Negara Malaysia has issued a circular “Outsourcing of Banking Operations” that allowed outsourcing of certain functions to external parties.

Main criteria for outsourcing are:

- Processes which are not integral to the core business,
- Outsourcing would not impair the image, integrity and credibility of the institution, and
- Lower cost for the institution to outsource, rather than developing the necessary infrastructure and expertise.

The following functions are allowed to be outsourced to external parties:

- Information systems internal audit,
- Credit card receivables collection, and
- Non-core operational functions.

15.1 Internal Auditors’ Role in Outsourcing Functions

Internal auditors should ensure the following basic principles are adhered to when reviewing an external party performing outsourcing functions:

- a. There must be a due diligence review performed to evaluate and ascertain the capabilities and expertise of the vendor prior to selection;
- b. Approval from the board of directors of the institution must be obtained and documented;
- c. The outsourcing vendor must provide a written undertaking to the institution concerned to comply with secrecy provision pursuant to Section 97 of the BAFIA;
- d. There must be a service agreement drawn up between the outsourcing vendor and the institution with a clause on professional ethics and conduct. The service agreement should also clearly define the roles and responsibilities of the outsourcing vendor;
- e. The service agreement should clearly state that the institution reserves the right to terminate the services of the outsourcing vendor if it fails to comply with the stipulated terms and conditions;
- f. There must be proper reporting and monitoring mechanisms in place to track the integrity and quality of work/services performed;
- g. There should be regular testing and review of work/services performed by the outsourcing vendor;
- h. Auditors, both external and internal, must be able to review the books and internal controls of the outsourcing vendor; and

- i. The institution must have a contingency plan to continue whatever work/services provided by the outsourcing vendor in the event the vendor is unable to continue. The contingency plan must be reviewed regularly to ensure the plan is current and relevant.

STUDENT PRACTICE 11

1. What is a business impact analysis in Business Continuity Plan? (para 12.1)
2. What is the minimum composition of a Shariah Committee in an Islamic financial institution? (para13(d))
3. What are some of the duties and responsibilities required of a Shariah Committee in BNM GPS 1? (para 13(f))

16. CONCLUSION

This chapter covers the audit of certain critical areas of a financial institution's operations and the minimum scope of audit work, which internal auditors must perform in the course of their audit. These critical areas of operations are not meant to be exhaustive. Therefore, internal auditors should also identify and review other operational areas deemed critical to specific businesses undertaken by the financial institution.

Appendix I: Main Types of General Insurance Coverage

Category	Coverage
Fire	Loss or damage caused by or arising from fire, lightning or domestic explosion.
Consequential Loss	Losses (as a result of fire) in earning power or profits due to partial or complete cessation, standing charges (i.e. those expenses that continue to exist after a fire) and increased cost of working.
Houseowner Insurance	Damage to private dwellings due to fire, lightning, explosion, impact by vehicles, bursting water tanks, theft or attempted theft, etc.
Householders Insurance	Loss or damage to contents of private dwellings against fire, explosion, impact by vehicles and theft if accompanied by forceful entry.
Marine Cargo	All risks of loss or damage to the cargo.
Personal Accident	Compensation for bodily injury or death caused by violent, accidental and visible means.
Group Hospitalisation and Surgical	Protects the employer against worldwide expenses incurred by an employee (and/or dependents) as a consequence of hospitalisation.
Burglary	Loss or damage to property caused by theft accompanied by actual, forcible and violent entry.
Money	Loss of money whilst in specific transits and while on the insured's premises.
All risks	Loss or damage due to accident or misfortune within the territorial limits.
Goods-in-Transit	Loss or damage to goods during transit anywhere within territorial limits.
Fidelity Guarantee	Protection for employers against the infidelity (dishonesty) of an employee causing direct financial loss.
Bond Insurance	A kind of contract in the form of a bank or insurance guarantee to accept responsibility for performance of a contractual obligation entered into by one party with another in the event of the former's default.
Workmen Compensation	Coverage to comply with s 26 of the Workmen Compensation Ordinance 1952 which lays out rules and regulations for the employer and his liability to insure his workmen. The law also lays down the scale of compensation which an employer is legally obliged to pay his employee or dependents as the case may be.
Public Liability	Protection for the insured for his legal liability to pay compensation for accidental bodily injury to or accidental damage to property of a member of the public caused by or through the negligence of the insured or his employees.
Professional Indemnity	Professional negligence due to a breach of duty of care owed by a professional to a client or third party arising in contract, tort or statute.
Motor	<ul style="list-style-type: none"> • 'Act' Cover – minimum cover indemnifying the insured for an unlimited amount for liability which may be attached to him in consequence of any third party being injured by use of the motor vehicle. • Third Party – 'Act' cover and indemnity for liability for damage of third party property. • Comprehensive – 'Act' and Third Party Cover plus physical damage to the insured vehicle following an accidental collision and also covers theft.

Appendix II: Main Types of Life Assurance Coverage

Category	Coverage
Whole Life Assurance	The sum assured is payable upon the death of the assured. Premium is payable throughout the life of the assured. However, such policies begin to accumulate cash or surrender value (after 3 years) which can be used for a policy loan, towards premium payment or early surrender of policy.
Endowment Assurance	The sum assured is payable in the event of death within a specified period of years, i.e. 15, 20, 25 or 30 years. However, if the life assured survives until the end of the period, the sum assured will still be paid. For the same amount of cover, the endowment assurance has the highest premium as it has the features of investments and/or savings which offer higher returns to the assured.
Term Assurance	i) <u>Basic Term Assurance</u> This policy offers basic life insurance coverage where the sum assured is payable upon the death of the life assured within the terms of the policy. Premium is payable until the end of the term (when the policy expires) or prior to death. There is no cash or surrender value. This policy can be converted into the permanent plan of assurance without evidence of insurability.
	ii) <u>Mortgage Reducing Term Assurance (MRTA)</u> A special form of term assurance designed to provide coverage to pay off the outstanding mortgage/loan owing to a bank in the event of the borrower's death. The sum assured will closely match the mortgage amount.