NCC Bank

नेपाल क्रेडिट एण्ड कमर्स बैंक लि.

Nepal Credit & Commerce Bank Ltd.

Internal Audit Policy

2072

2016

Table of Contents

Internal Audit Policy

1. Internal Audit Policy

This internal audit policy sets out the principles under which Internal Audit Function has to operate within Nepal Credit & Commerce (NCC) Bank Ltd. The Audit Policy of the bank shall clearly enumerate the policies of the management in respect of Internal Audit functions in all the functionaries of the bank. This policy is a governance policy, which should be followed for all work undertaken by Internal Audit Department.

BASEL Accord issued by NRB has upheld the significance of internal audit function in banks. It has emphasized on efforts to harmonize and improve internal audit standards to align it with international standards. It has recognized internal audit as a part of the on-going monitoring of the bank's system of its internal control and of its internal capital assessment procedure. Also, it has emphasized that internal audit should focus on risk monitoring and risk mitigation.

2. Objectives of Internal Audit Policy

i) To examine & provide high quality counsel to management on the effectiveness of risk management procedures and internal control system including regulatory compliance by the bank;
ii) To provide an objective and independent assessment of line management's activities and stewardship of the businesses;
iii) To examine the economy, efficiency and effectiveness of operations including non-financial controls of the bank;
iv) To enable the organization to initiate necessary measures to protect it from any future hazard;
v) Have regard to the materiality of risk when reviewing and reporting on the activities of the Bank and prioritize its own work in the same manner;
vi) Ensure that internal audit supports the control environment in a better shape ;
vii) Be a part of the accountability review process in the event of any major control failure within the bank's businesses;
viii) Maintain and operate professional as well as structured risk based internal audit methodology, which shall govern the international best practices;
ix) To follow-up for rectification of irregularities pointed out in the Audit Reports for corrective actions and get confirmations from Controllers regarding rectifications of irregularities;
x) To take responsibility for promoting a high level of internal control awareness throughout the Bank;
xi) To establish a structured organization, system and framework for generating credible assurance to stakeholders;
xii) To rectify the operational errors observed during the course of on-site audit instantly and educate the staff members in order to stop the repetition of same types of errors in future;

3. Handling of Internal Audit Policy

This policy is intended for the Bank's internal use only and remains the property of NCC Bank Limited. No part of it should be made available to outside parties without approval from the CEO.

The head of the Internal Audit Department and all other departments have a responsibility to ensure that such duty of confidentiality is upheld at all times by them as well as by the staff under him/ her. The auditing staffs must maintain the confidentiality of information acquired and exercise with professional ethics while performing audit functions.

4. Internal Audit

Internal Audit is an independent appraisal to determine whether acceptable policies and procedures are being followed, whether established standards are being met and whether resources are being used efficiently and economically to achieve the objectives of the organization. It is an essential established tool for control and feedback for proper risk management and governance of the organization.

5. Vision/ Mission of Internal Audit Department (IAD)

Mission of IAD

To enhance the capacity of NCC Bank Limited to make impeccable decisions for the achievement of the overall organizational VISION by implementing the norms of corporate governance and by strengthening the mechanism for monitoring and managing various risks (Credit, Operational, Liquidity, Foreign Exchange, Regulatory, Reputational, and Market, etc) and to establish the strong reporting system to minimize the banking risks so as to protect legitimate interests of all stakeholders.

Vision of IAD

To offer standard Audit services in an independent manner and assure financial and operational integrity, accountability, efficiency, effectiveness and Compliance Service to the NCC Bank Ltd.

6. Objectives of Internal Audit

The objectives of Internal Audit will broadly cover:

1) To examine and evaluate whether the bank's framework of risk management, control and governance process is adequate and properly functioning in congruent with overall long term business strategy of the bank.
2) To advise and recommend the management and Board of the Bank for improving internal control and risk management system.

Other Objectives are as follows:

1) Examination and Evaluation of the adequacy and effectiveness of the internal control systems of various operational activities of the Bank;
2) Review of application and effectiveness of risk management procedures and risk assessment methodologies at various operational activities of the Bank;
3) Preparation of Risk Audit Matrix based on intensity/ magnitude and frequency of risk;
4) To act as value adding unit rather than the fault finding unit;
5) Review of management and financial information system including electronic information systems and electronic banking services;
6) Review of the accuracy and reliability of accounting records and financial information system;
7) Testing of both transactions and functioning of specific internal control procedures at various departments of the Bank's branches and departments;
8) Review of the system established to ensure compliance with legal and regulatory requirement, code of conduct and the implementation of policies and procedures;
9) Evaluation of effectiveness of existing policies and procedure and to give recommendations for improvements;
10) Identify the opportunities for cost savings and making recommendations for improving cost efficiencies;
11) Review of the means of safeguarding the assets;
12) Carryout investigation assigned specifically and/ or on the basis of audit result;
13) Confirm that the directives issued by NRB are strictly adhered to;
14) Confirm that loan loss provisioning is adequate and not inflated to create secret reserve;
15) Confirm that the Financial Statements disclose the Bank's financial position correctly;
16) Follow-up on the implementation of the external auditor's and NRB inspector's report;
17) Other as prescribed by the Audit Committee from time to time;

7. Provisions laid down on NRB Directives for Audit Committee, Internal Audit, and Control

NRB Directives no. 6 and 7 have dealt with:

i) Corporate Governance, and
ii) Internal Audit & Control

Directive no. 6, inter alia, deals with the arrangement relating to establishment of an Audit Committee of the Board under a non-executive Director. It states that:

The Board of Directors of the licensed institution shall establish an Audit Committee under a non-executive director. This committee shall review the institution's financial condition, its internal controls, audit program, and upon detailed discussion on the findings of the internal audit, shall issue necessary guidelines to the management of the institution. The external as well as internal auditors

shall have free access to this Committee. The Board of Directors of the licensed institution shall discuss in detail the reports of the auditors and the Committee. The Chief Executive Officer shall not be included as the member of the Audit Committee formed by the licensed institution. However, this shall not prohibit from including him/ her as an invitee, whenever necessary.

The following as prime responsibilities of the Audit Committee:

1) To review the licensed institution's financial condition, internal controls, audit program, and findings of the internal audit team and to recommend to the Board of Directors about the actions to be taken;
2) To review the matters contained in the audit report of the external (statutory) auditors and initiate for necessary corrective actions;
3) To review the matters contained in on-site inspection report provided by Nepal Rastra Bank and furnish the implementation status regarding the observations/ remarks/ directions to the Board of Directors of the bank;
4) To help ensure publication of annual report in true and accurate manner;
5) To assure the Board of Directors that accounts are accurate and fair, along with frequent reviews of the adequacy of provisioning against contingencies and classified loans;
6) To review the compliance of the regulations issued by Nepal Rastra Bank to the licensed institution and include the same in its report;
7) To ensure the audit activities of the branches and departments of the bank have been performed as per 'Annual Audit Plan' approved by the committee;
8) To review the activities of licensed institution in respect of its regularity, economical, logical, effectiveness, and give necessary suggestions to the Board of Directors;
9) To review the financials of the bank in quarterly basis and submit the report to the Board of Directors of the bank;
10) To perform the functions stipulated in Section 165 of Company Act 2063;

Internal Control System stated on NRB Unified Directives 2072 no. 7 is as follows:

The licensed institution shall develop procedures designed to ensure effective internal control systems that make sure that the employees are performing their duties in accordance with the existing policies and procedures, as well as the law. The procedures, at the minimum, should include the following:

1. Procedures to review management and accounting controls that protect the value of institution's assets and provide a true picture of the condition of the licensed institution.
2. Procedures to verify the reliability of the statistics.
3. Procedures for verifying the application of policies with respect to the extension of credit, treasury operations, foreign exchange management, liquidity management, capital adequacy, human resources, management information systems as well as compliance of banking laws and regulations.
4. Procedures for assets quality review.

5. Procedures for review of financial risk management (liquidity, assets/ liabilities, foreign exchange management).

Other scope of work of the Audit Committee:

1) To review the reports presented by Internal Auditors and instruct the management on the basis of findings of the report.
2) To present/recommend before the BOD of the Bank on following matters:
   a) Serious issues raised/ cited in the report of the Internal Auditors of the bank.
   b) Audit remarks/ issues raised in Investigation Report leading to take action to staffs of the bank.
   c) Preliminary report and final report presented by the external (statutory) auditors of the bank.
   d) Financial position, internal control situation, internal audit plan, branch expansion program and other relevant policy matter reported by the Internal Auditors of the bank.
   e) An assessment on contingent liability, loan classification and adequacy of loan loss provision.
   f) Other relevant matters which help to strengthen internal control; maintain/ improve corporate governance and transparency in the bank.
3) To advise the management for the operation of the Bank in the most efficient and competitive manner.
4) Other important matter as directed by the board.
5) Other matters as stipulated in NRB directives and other regulations.
6) To report and recommend to board about the pertinent issues with regard to mitigate risks and strengthen the efficiency, internal control, corporate governance etc. for the better and effective management of bank's operation/business.
7) Responsible for developing and maintaining a secure, confidential and effective whistle-blower mechanism inside the bank for reporting and investigation of allegations of suspected improper activities.

8. Strategies to achieve Objectives of IAD

1) Maintaining independency and transparency while conducting audit function.
2) Preventive and Proactive, rather than detective and reactive approach of auditing
3) Systems and Procedures for different audit processes (involving pre-audit, audit and post audit) will be standardized and codified to the extent possible to infuse objectivity and uniformity into the Internal Audit System. Periodic review of the systems and the procedures including Audit Report Formats and existing Procedural Manual – Internal Audit Department will be undertaken to respond to the emerging risks which the bank has been exposed or likely to be exposed.
4) Assisting in the development and implementation of effective policies and procedures and educating all concerned about the provisions of various policies/ procedures/ guidelines adopted by the bank and regulatory environment (for implementing the proactive approach to auditing)

5) Finding out causes and the remedies along with findings
6) Reviewing the decisions made so that control, and compliance considerations could be taken care of in time
7) The audit of the branches and departments will be conducted within the outer limits of the prescribed periodicity. While deciding the periodicity, nature and group of business, the risk profile of the auditee units and the regulatory guidelines issued from time to time will be taken into account.
8) As an ongoing for strengthening the audit culture, self assessment by the branches and departments is mandatory for assessing their strengths and weakness and their risk profile.
9) Apart from the normal audit or full-fledged audit of a unit/ branch, IAD may undertake the audit of any or more specific aspects or areas or transactions at its discretion or in response to specific demands from the management for conducting such an audit.
10) Constantly monitoring the needs for updating the systems, policies, and procedures adopted by the Bank in the light of experiences and feedback received during the course of implementation so that the systems, policies, and procedures adopted by the bank continue to be effective, relevant, and practicable;
11) Appropriate strategies will be adopted by IAD to ensure audit functions remains cost-effective and minimum disruption to the auditee unit is caused.
12) Auditee unit/ controller shall be responsible for creating conducive environment for audit and furnishing required information to the audit team.
13) Obtaining feedback from all concerned on the ways and means to improve the system and achieve greater effectiveness and efficiency.
14) In order to control the fraud and significant deviations from legal/regulatory/procedural norms, a proper mechanism shall be developed into the bank. Every employee is encouraged to provide such information through this mechanism directly to Secretary to Audit Committee. Such information shall be kept confidential and no any disciplinary or other action shall be taken against information provider.
15) Communicating to audit committee about the relevant issues and audit report to take the timely corrective action, if any, and to address the remarks by concerned branch/department through oversight of IAD.
16) Continuously monitoring the risk in different operational areas of the bank and recommend to audit committee/management of the bank to take necessary actions in order to mitigate the current and potential risks in bank's operation and management.
17) Any other strategies and actions which helps to enhance the efficiency and independency of internal audit department.
18) Promoting the concept of self audit system

Guiding Principles in the selection of Audit Procedures

1. Effective in the achievement of the set objectives
2. Efficient in the utilization of the resources (guided by priority)
3. Proactive in the prevention of frauds and errors

4. Fair and Objective in conducting the audit and reporting the findings thereof
5. Inquisitive, Receptive (open minded) , and Cooperative
6. Adopting international best policy and practices to conduct audit functions

9. Authority of the Head of IAD

The authorities of the Head of the Internal Audit Department include the followings:

a) Unrestricted access to all departments, offices, activities, records, information, properties, personnel, etc. as deemed necessary and relevant for the purpose of conducting audit;
b) Applying any techniques of auditing, as may be necessary to accomplish the audit objective;
c) Obtaining necessary assistance of personnel in various departments/ offices of the Bank where the audit is being performed;
d) Obtain assistance of specialist where considered necessary from within or outside the Bank;
e) Other authorities as delegated by the Audit Committee

10. Responsibility of the Head of IAD

To provide an objective evaluation of internal control system put in place by management, every aspect of the business and operations of the Bank may be subject to audit. In keeping with the role of the IAD, the head of the IAD will be accountable but not limited to following core responsibilities:

a. Co-ordinate and provide support and oversight of all external auditors and regulators, as appropriate, for the purpose of providing optimal audit coverage;
b. To develop a flexible annual audit plan using an appropriate risk based methodology, including any risks and control concerns identified by management and submit the plan to Audit Committee for review and approval;
c. Implement the annual audit plan, as approved, including any special tasks assigned by the Audit Committee;
d. Should have regard to the materiality of risk when reviewing and reporting on the activities of the bank;
e. Ensure that audit leaves the control environment in a better shape than existed prior to an audit engagement;
f. Be a part of the accountability review process in the event of any major control failure within the businesses;
g. Maintain a professional and structured audit methodology, which is well regarded by the regulators and external auditors;
h. Take responsibility for promoting a high level of control awareness throughout the bank;
i. Encourage all staff to adopt the system/ procedures of self - audit and promote compliance culture;
j. Communicating in timely manner about relevant issues of the audit observations, findings, remarks, reports etc to audit committee
k. To follow-up the previous audit reports and compliance thereof.
l. To maintain the confidentiality of relevant issues and put those issues to concerned authority or in audit committee.

The other responsibilities of the Head of Internal Audit Department include the following:

a) Maintain requisite professional audit staff strength with sufficient knowledge, skills, experience, and professional qualifications to meet the objective of the bank.
b) Issue periodical report on timely basis to the Audit Committee summarizing results of audit activities.
c) Keep the Audit Committee informed of emerging trends and developments in internal auditing practices and give recommendations for necessary revisions in this policy.
d) Conduct investigation of significant suspected fraudulent activities and notify the results to Audit Committee and related competent authority of the bank.
e) Ensure that the department complies with sound internal auditing principles and best practices.
f) Review and certification of Statutory Requirements, such as, Capital Adequacy Ratio, Financial Highlights of the bank, information to be delivered in the quarterly reports etc. The transactions and reports related to Anti-Money Laundering/ KYC, LC, INR/ other Foreign Currency Draft/ T.T/ SWIFT Issuance, Good for Payment etc. shall be scrutinized.
g) Other duties and responsibility as assigned by Audit Committee, etc.

11. Accountability, Independence, and Conflict of Interests

An auditor must always be independent. This extends beyond mental attitude, so that the auditor is seen by others to be independent. In order to avoid conflict of interest, employees working in Internal Audit Department will not simultaneously be involved in other operational duties not compatible with Internal Audit Function.

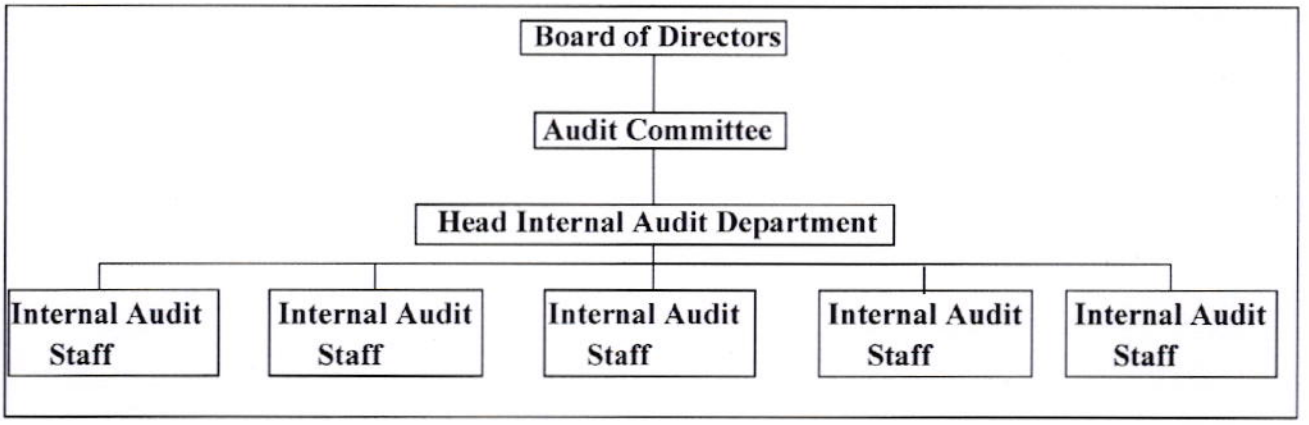
Auditors have no line responsibility or authority over any of the operations they examine. This is to ensure the independence necessary for the Internal Auditor to exercise judgment, express opinions and present recommendations impartially.

a) The Head of the IAD is accountable to the Audit Committee.
b) To maintain the independence of the Internal Auditors, the head of the IAD shall report to Audit Committee and upon the instruction of Audit Committee, a copy of reports shall be forwarded to CEO.
c) Internal Audit Department will be independent of the activities of the auditee. The department will also be independent from the internal control process of the bank.
d) Internal Auditors shall exercise their assignment on their own initiative in all departments, offices and branches of the bank.

12. Organization & Internal Audit System

Internal Audit is a permanent function; its continuity should be ensured. It must have independence, impartiality and professional competence approach. Audit Committee is in place and functions as per NRB guidelines. The Bank already has an Internal Audit Department as a tool for internal control and feedback to the management as well as to the Board through the Audit Committee of the Board.

Internal Audit Department shall be set up under the Head - Internal Audit Department.



During the course of time, depending upon the workload, the bank will build up sufficient manpower in the Internal Audit Department to conduct various types of audit as per their policy.

The Head of Internal Audit, to whom they would report, would supervise their work.

The Head of Internal Audit would report to the Audit Committee of the Board and will act as Member Secretary of the Audit Committee.

Performance appraisal of Head of Internal Audit Department will be carried out by the members of Audit Committee whereas the performance appraisal of other staff members of the department shall be conducted by Head of Internal Audit Department and submit to Audit Committee for necessary review.

Internal Audit Department will organize, in coordination with the Human Resource Department, appropriate briefing/ training to the audit officials to ensure that they discharge their duties effectively/ skillfully.

Internal Audit Department will standardize inspection procedures and develop rating parameters of branches/ portfolios reciprocate to Risk Matrix in line to regulatory requirements in need based manner.

13. Internal Audit Coverage

Internal Audit would cover audit of Credit facilities including Letters of Credit, Guarantee, Deposits, Remittances, Treasury, Forex, Reconciliation, Cards Division, Human Resources, General Administration, Credit Administration, Share, Legal & Recovery, Finance & Planning, Compliance, Fixed Assets, Security, System Management & IT, various units engaged in processing of instruments/ documents or managing operational activities, new products and services, etc.

In addition to the above mentioned regular audit of departments/ branches, the department shall carry out various types of other activities, such as:

a) Concurrent Audit
b) Review of Corporate Governance
c) Surprise Audit/ Visit etc.

The regular audit of Information Technology & System of the bank is to be covered under **'Framework on Information System – (IS) Audit**, which is in place and approved by Audit Committee **(Annexure 1)**. Also, the management should assess the need of **System Audit** by outsourcing the audit function for minimizing the operation and IT or system related risk of bank.

An Annual Audit Plan would be drawn up by the Head of the Internal Audit for each Fiscal Year and this would be put up to the Audit Committee for approval.

Spot/ specific audit may be arranged by the Head of Internal Audit on being advised by the CEO or instructed by the Audit Committee, the Board of Directors or the Regulators. The Head of Internal Audit may also initiate specific audit with the approval of the Audit Committee.

Status report on the implementation of Annual Audit Plan as approved shall be put up in each Audit Committee meeting.

14. Principles & Methodology

The internal auditors should comply with ethical principles governing professional responsibilities. (Para 6-7 of Nepal Standard on Auditing – 1.Ethical principles governing the auditor's professional responsibilities are:

Integrity, Objectivity and Independence:

The internal auditor should be straightforward, honest and sincere in rendering professional services. The auditor must be fair and should not allow prejudice, bias or influence of others to override his/ her objectivity. The auditor should maintain an impartial attitude and both be and appear to be free of any interest which might be regarded, whatever its actual effect, as being incompatible with integrity, objectivity and independence.

Integrity:

Establish trust and thus provide the basis for balance on the judgment of Internal Audit. Remain tactful, honest, objective, diligent and credible in all relationships.

Objectivity:

Exhibit the highest level of professional objectivity in gathering, evaluating and communicating information when they are being examined. Make balanced assessments of all the relevant circumstances and do not become unduly influenced by individual interests or by other in forming judgments.

Independence

Maintain independence without taking direct responsibility or any authority over the activities or operations.

Professional Competence and Due Care:

The internal auditor should apply the knowledge, skills and experience needed in the performance of internal auditing services and continually improve their proficiency and the effectiveness and quality of their service.

The internal auditor should perform professional services with due care and competence and has a continuing duty to maintain professional knowledge and skill at a level required to ensure that the Unit/ Branch receive the advantage of competent professional service.

Confidentiality:

The internal auditor should respect the confidentiality of information acquired during the course of performing professional services and should not use or disclose any such information without proper and specific authority or unless there is a legal or professional right or duty to disclose.

Professional Behaviour:

The internal auditor should act in a manner consistent with the good reputation of the profession and refrain from any conduct that might bring discredit to the profession.

Technical Standards:

The internal auditor should carry out professional services in accordance with the relevant technical and professional standards. Auditors have a duty to carry out with care and skill, instructions of clients insofar as they are compatible with the requirements of integrity, objectivity and independence.

15. Risk Focus and Risk Mitigation

Internal audit should focus on the various risks arising from the environment vis-à-vis various kinds of operations/ activities undertaken by the bank and risks arising from deviations from the established laws, directions, Policy Guidelines approved by the Board and Management Instructions in the form of Circulars or in recorded notes.

Risk is defined as the probability of an unexpected loss due to unexpected change of position and environment. Risk is inherent in banking/ financial transactions. Many banks have faced huge losses and hardship due to their failure in identifying risks and failure in putting in place systems to mitigate the risks.

Internal Auditors should identify and report on the various kinds of risks and should also indicate wherever necessary, the level thereof (High/ Medium/ Low) to which, the Bank may be exposed or

might have been exposed in course of various operations/ activities.

16. Compliance

Compliance is concerned with the legality and integrity of the business activities. Internal Audit Department should help management to ensure that the bank operates to the highest standards and meets all regulatory and legal requirements.

17. Internal Audit Plan

Internal Audit planning process is an important stage as it directs limited resource of audit team towards effective utilization to achieve audit objectives. Therefore, it is essential that adequate exercise be done at this stage in order to ascertain frequency and depth required for inspection of a particular department, division or branch.

Internal Audit Plan shall be drawn up at the beginning of each Fiscal Year keeping in view the following but not be limited to the items mentioned below.

i) NRB Directives on verification audit on Import Letters of Credit
ii) Other NRB Directives on audit coverage (Compliance Audit)
iii) Organization structure of the Bank
iv) Branches/ Units/ Departments of Corporate Office to be audited
v) Review of bank's performance in comparison to the budget allocated
vi) Frauds and Abuse Investigation
vii) Directions from the Audit Committee and from the Board to the Internal Audit Department

18. Internal Audit Procedure

In order to carryout effective internal auditing of any department/division/branch of the bank, it is essential to understand the workflow and function of such branch/office. The audit procedure mentioned below will enable the staffs of IAD to better understand the function of the department/ division/branch and recognize control measure, which may be required to check to carry out the verification procedure. The Internal Auditors shall focus on:

i) Credit risks, Credit Concentration Risks
ii) Operational risks (inherent in all operations including credit)
iii) Liquidity risks
iv) Market risks
v) Foreign Exchange risks
vi) Regulatory risks (non-compliance of GON/ NRB Directives in various operations)
vii) Interest rate risk that is reviewed and looked after by Asset Liability Management Committee (ALCO).
viii) Internal Capital Adequacy Assessment Process (ICAAP) of bank
ix) Compliance risk
x) Reputation risk
xi) Strategic risk
xii) Other prominent risk that to be faced during the execution of bank's day to day activity

Bank's officials, particularly the Senior Management would be responsible for developing processes to identify measure, monitor and control above risks. However, the Internal Audit Department shall provide the appropriate information that observed by them during the course of audit in time in order to facilitate the senior management to control the risks. The information provided by the Internal Audit Department shall serve as a basis for Management decisions and bank control.

Internal Audit Process

a) **Plan:** Develop an audit plan based on a review of all pertinent information. Sources may include prior audit work papers, prior audit reports, policy manuals, risk assessment matrix etc.
b) **Notify:** Schedule a meeting with the Head of Auditee unit, Identify the scope and objective of the audit, duration of the audit
c) **Test:** Test will include interview with the staff. Review of procedures and manuals, compliance with the bank policies and regulations and assessing the adequacy of internal control
d) **Communicate:** Communicate the audit findings/ recommendations
e) **Draft:** The draft report shall be sent to respective auditee unit for necessary information
f) **Management Response:** Time limit to be mentioned for the response of the management
g) **Review:** The final report to be reviewed by the Head, Internal Audit Department
h) **Distribute:** Auditee Unit, Audit Committee and others as instructed by Audit Committee
i) **Verify/ Follow up:** Follow up of the audit remarks

19. Internal Audit Report: Objective, Basis for Verification & Structure

The Audit Report, as a document, facilitates audit activity to achieve overall audit objectives.

Audit Report is the basic document to provide vital feedback to the concerned branch/ unit as well as to the senior management, CEO and to the Board through the Audit Committee. It is very important for any auditor to understand that based on the audit report, the users shall take future course of action to strengthen the internal control procedures and adopt risk mitigation measures.

Books and accounts of the bank, vouchers, documents, completed forms, notes, written instructions etc. shall generally form the basis for verification with reference to the laws of Government of Nepal, NRB Directives, Manuals of the Bank, Policy Guidelines approved by the Board, Board decisions and decisions of other committees of the bank, Circulars issued by the management and probable risk of loss.

Auditors shall also recheck on the last audit and inspection reports of the Internal Auditors, Statutory Auditors and NRB Inspectors to ascertain improvements or deterioration of the state of affairs reported earlier.

Reports should not contain too much of procedural and theoretical details. It should be objective, risk focused, precise and cover both policy and procedural aspects.

In respect of audit reports on units/ branches, efforts shall be made to present a realistic and constructive pictures by commenting on the profile of the unit/ Branch, quality of customer service, premises and upkeep, security arrangement, business profile and focus if any and on achievement vs. potential.

20. Procedural Manual – IAD, Audit Checklist & Program

The procedural Manual of the bank covers the areas of Concurrent Audit, Off-site Inspection, On-site Inspection (Operation Department, Treasury & Fund Management Department, Human Resource Department, General Administration Department, System Department, Trade Finance Department, Credit Risk Department, Cards Department, Branch Operation Department, Credit Administration Department and Finance & Planning Department) to be followed while conducting audit & inspection of branch/ department. However, Internal Audit Department shall incorporate bank policies/ manuals/ guidelines as well as circulars/ directives issued by the bank and regulator in addition to the scope cited therein.

Likewise, audit programs and audit checklists may be prepared to enhance the efficiency and effectiveness of the Internal Audit Function and to facilitate effective implementation of the annual audit plan. The Audit Committee shall approve the annual audit plan prepared by the head of the Internal Audit Department with or without modification. However, approval of the Audit Committee is not necessary for the audit programmes and audit checklists.

The Audit Committee may issue necessary instructions, from time to time, regarding the format of the audit reports, audit plan, audit program, audit checklists, audit frequency, audit coverage, or audit procedures, etc. to the head of the IAD. It shall be the responsibility of the Head of the IAD to conform to the instructions/ directives of the Audit Committee at all times.

21. General Guidelines for Preparation of Audit Report

The Internal Audit Report should include the following:

- Background information on the organisation unit and activities reviewed.
- Whether the Audit was undertaken in the response to a scheduled engagement (as per the Audit Plan) or in response to appropriate instructions.
- Engagement objectives
- Engagement period
- Review period
- Activities reviewed or not reviewed should be clearly identified and stated to describe the boundaries of engagement
- Observations, conclusions, opinions, recommendations and action plans
- Executive summary for overview by the Audit Committee
- Repetition of similar remarks/comments as mentioned in previous reports.

Internal Audit Report shall cover several areas of operations or a number of loan files. It is essential that suitable audit observations are recorded on each area of operation or on each loan account audited.

In the case of loan accounts, the audit observations should invariably be presented precisely at the end of each account reported and if there are no observations/ issues for action, it should also be stated accordingly. A summary of these may be mentioned in the Executive Summary.

The final audit report is required to be submitted to the Audit Committee by the Head of Audit Department. It shall be sent to the Branch Manager/ In charge of the audited branch/ department both in soft copy for response. Upon receiving quick response from the branch/ department audited, the reports shall be submitted to Audit Committee for their deliberation and instructions. The Audit Committee meetings take place at periodical intervals.

22. Performance Evaluation & Reporting

Discussions shall be made with the Chief/ In-charge of the audited unit/ department before finalization of the audit report. The discussion shall be both informal and written during the course of audit. The discussion shall focus on taking the corrective measures for the observations and remarks noted by the audit team.

The auditor should present himself/ herself as a facilitator rather than a detective in order to work hand in hand with the auditee unit/ Department officials so that they do not perceive the auditor as corporate police and provide honest and open feedback for improvement in the areas of concern and also in their response on the audit report. The auditor should educate the employees of the auditee unit/ department to correct the remarks observed which will enable to build up proper rapport during the audit engagement.

The draft audit report should be invariably discussed and the position in this regard should be clarified in the audit report. Further, minor irregularities, if not rectified and re-appear in the subsequent audit verification should be considered as major.

Prompt and effective implementation of the Internal Audit Reports leads to risk mitigation and changes in policies and procedures where needed and enhancement of internal control system of the bank.

Minutes of the Audit Committee meetings are submitted to the Board. A copy of the minutes may also be furnished to the CEO for necessary action.

Extracts of the minutes are furnished to the Head of Branch/ Department/ Unit audited and action points are followed up till the item is disposed off and reported to the Audit Committee.

Implementation (Disposal) of the Internal Audit Reports by the Branches/ Departments concerned is kept under review by the Internal Audit Department and Status Report is submitted in the Audit Committee meetings.

All audit reports will be made available to the Auditee unit, Controller and concerned Department with a copy to Internal Audit Department. However, copies of special reports will not be made available to the auditee unit to maintain/ ensure confidentiality in the matter.

All the Internal Audit Reports issued, and gist of all Special Purpose Audit (Flash Report, Spot Audit, Special Investigation etc.) reports, if any, submitted by the Internal Audit Department to the management, shall be submitted to the Audit Committee in its meeting held immediately after the issuance of the report.

23. Reporting Requirements

The Head of the Internal Audit Department is required to report directly to the Audit Committee of the Bank and forward a copy to CEO. He/ She is required to cover the following aspects in their reports:

On Quarterly Basis

1. Major remarks/observations of the Internal audit reports on branches/offices of the Bank, comments from the concerned office and recommendation of the Department.
2. Brief report on the investigations (if any) conducted by the Department.
3. Comparative performance of the Bank (Balance Sheet, Profit & Loss Account, together with loan classification, provision for possible loan losses and contingent liabilities of the Bank).

On Annual Basis

1. Annual Audit plan
2. Important Improvements and uncompleted tasks raised/ commented in internal audit report, external audit report and NRB inspection report.

When the head of the IAD submits its report of the audit activities to the Audit Committee, it will provide among other issues an independent assurance to management and to the Audit Committee i.e.:

- The risks associated with all aspects of the Bank business and operations have been identified,
- An effective system of controls over these risks is in place and is working as intended,
- The Bank's plans, policies and principles have been effectively communicated and implemented.

Upon review of the internal auditor's report, it shall issue necessary guidelines/ instructions to the management. This will also reinforce an independent role and responsibilities, avoid any influence by higher-level officials over the judgments and opinion expressed by the Internal Auditor.

24. External Auditors

The external auditors will have access to Bank information; however, the Head of the IAD should be taken in confidence prior to providing such information to an external auditor. An external

auditor should be able to rely on Internal Audit Department's work to the extent that it is focused along similar objectives, and acknowledge Internal Auditor's independence and the quality work. This process enables the cost and time of the external audit to be reduced. Similarly, the Internal Auditor can use the work of the external auditors as part of the continuous risk assessment process, and rely upon the aspects of their work, which relate to statutory obligations. Each year the Board will appoint external auditor(s) during Annual General Meeting.

Internal Audit reports may be made available to the external auditors and they can review and examine the reports / files within the scope of our audit policy. However, they should not be allowed to take the files outside the Bank's premises.

25. Regulators

The regulators can enquire and demand Bank's information or wish to have access to Bank's records. Whilst the Bank has to accede to their request, no information or files may be sent to external regulator(s) without taking the Internal Auditor in confidence or without the express approval of concerned authority. The external regulator(s) should rely on Internal Auditor's work to the extent that it is focused along similar objectives, and acknowledge Internal Auditor's independence and the quality of work. A close working relationship should be maintained at all times with the regulators to ensure efficient running of the Bank.

26. Applicability

The policy shall be applicable immediately upon approval by the board.

27. Improvements / Revision to the Internal Audit Policy

It will be a continuous process to refine and streamline the audit process to suit the best practices. Based on practices and the operating environment, Head of IAD will put up the proposed revision to the meeting of the Audit Committee. The audit policy shall be subject to review and modification as and when necessary and at least once in every two years by obtaining feedback/ suggestions from the CEO, top functionaries in the management and from the Internal and External auditors by the Audit Committee. Further, The Audit Committee makes decision regarding the improvement/revision after considering the following factors:

- Combine the ability to detect all major control weaknesses and minimize related control failures
- Support and guide business unit in managing various risks and achieving their objectives
- Will be well regarded by the regulators
- Practical matters, which will come in light, will be addressed

This internal audit policy has been made to make consistent with NRB Directives issued from time to time, Company Act 2063, Banks and Financial Institutions Act 2063. In case of any disputes/ contradictions arises in provisions contained in this policy and those contained in the directives issued by NRB, the latter shall prevail.

Annexure 1: Framework on Information System – (IS) Audit

Information Systems (IS) Audit

Summary

The business operations in the banking and financial sector have been increasingly dependent on the computerized information systems over the years. It has now become impossible to separate Information Technology (IT) from the business of the banks and the financial institutions. There is a need for focused attention on the issues of the corporate governance of the information systems in computerized environment and the security controls to safeguard information and information systems. The banking industry is responsible for implementing effective security controls to protect information assets as confidentiality, integrity, authenticity and availability of such information is of utmost importance to business operations. Strategically planned and implemented information infrastructure is not only scalable but also provides efficient operations to meet the need of the future business requirements. The primary objective of the information system audit is to identify performance bottlenecks, security holes and security control gaps in the bank.

Introduction

The application of Information Technology has brought about significant changes in the way the institutions in the banking and financial sector process and store data and this sector is now poised to countenance various developments such as Internet banking, e-money, e-cheque, e-commerce etc., as the most modern methods of delivery of services to the customers. The telecommunication networks have played a catalytic role in the expansion and integration of the Information Systems (IS), within and between the institutions, facilitating data accessibility to different users. In view of the critical importance of IS, there is a need to exercise constant vigilance for the safety of the financial systems. Structured, well defined and documented security policies, standards and guidelines lay the foundation for good IS security and each institution is required to define, document, communicate, implement and audit IS Security to ensure the confidentiality, integrity, authenticity and timely availability of information, which is of paramount importance to business operations.

The information systems security has greater importance for the commercial success of an organization as the survival of the organization depends on the speed, accuracy and reliability of the flow of information within the organization vis-à-vis its customers.

The security controls are required to minimize the vulnerability and to prevent unauthorized use of the information and the information systems. However, such controls may have to be consistent with the degree of exposure of such system and the information and the impact of loss to the organization on account of unauthorized access and misuse, including accidental misuse, of such systems and information. The unauthorized use and access including accidental misuse of the information may result in financial loss, competitive disadvantage, damaged reputation, improper disclosure, law suits and non-compliance with the regulatory provisions.

As the bank is responsible for implementing the effective security controls for protecting information assets, it must perform detailed and comprehensive audit of Information Technologies including hardware, software and processes and security controls. The staff designated for System Audit is positioned to provide this support to the bank.

Constant vigilance and the extensive and proper implementation of the information systems security program in an organization are the minimum requirements for the organization's competitiveness and continued contribution to sustainable business growth.

Objectives

The main objective of Information System (IS) Audit is to evaluate and report on IT security architecture, Information System resources and infrastructure. The assessment shall focus on the bank's critical internal systems and the evaluation of operating effectiveness of controls that are currently in operation to safeguard Information System Assets.

Staff Information System Audit to assess:

1) IS Security/ Controls relating to computer hardware, software, network, Telecommuting/ Tele-working, Mobile Computing, Computer Media Handling, Voice, Telephone and related equipment and Internet and the procedures/ methodologies to be adopted to safeguard information and information systems.

2) Bank's information assets are secured against unauthorized access/ usage/ damage/ changes

3) Bank's business continuity planning is adequate enough to ensure customer service, despite interruption to technology facilities for a significant amount of time

4) Precisely identify bank's technology infrastructure as well as users at any given time frame are adequately protected that bank's computer operations are carried out in a controlled environment

5) Capacity management of bank's ICT infrastructure is optimized (right sized) to deliver services effectively and efficiently

6) Assurance over effectiveness of controls exercised by out-sourced vendors for technology services

Detail Scope of Audit

1. Core Banking System
    a. Input, Processing & Output controls
    b. Logical access controls
    c. Controls over automated processing/ updating of records, review or check of critical calculations such as interest rates, etc. review of the functioning of automated scheduled tasks, output reports design, reports distribution
    d. Functionality & Parameter Setting
    e. Internal control built in at application software level, database level, OS server level.
    f. Back-up/ Fall back/ Restoration procedures and contingency planning
    g. Suggestion on segregation of roles and responsibilities with respect to application software to improve internal & Change controls
    h. Review of documentation for formal naming standards, design process for job roles,

activity, groups and profiles, assignment, approval and periodic review of users profiles, assignment and use of super power access

i. Manageability with respect to ease of configuration, transaction roll back, time taken for end of day, day begin operations and recovery procedures
j. Adherence to legal/ statutory requirements
k. Review of risk control measures in core banking interfaces like interface in CBS with Nepal Clearing House Limited and others if any.

2. Internet Banking and other Applications
    a. Review and report on the overall Information Systems Security Framework for internet banking including security aspects of the entire Internet Banking Architecture with recommendation for improving the security if any
    b. Review and suggestions for improvement in the security policy, security/ vulnerability patches, adequacy of tools for monitoring systems and network against attacks
    c. Review of risk control measures on legal/ statutory requirements and private policy with special reference to internet banking scenario
    d. Money Transfer Payment process and application
    e. Mobile Payment process and application
    f. Procedures for opening and operating accounts with thrust on legal aspects in Internet Banking & Maintenance of records in internet banking scenario

3. Web server/Mail server/Application server/ DB server/ File server
    a. Configuration of Mail, Web, Database and file servers
    b. Security settings with reference to security policy
    c. Security patches applied are current/ latest
    d. Exposure of sensitive data on public area
    e. Ports on need to have basis, with special thrust on disabling unnecessary ports or ports that are potentially risky
    f. Usage of 'Super User' account

4. Activity Logs
    a. Review and report on adequacy of audit logs and procedures for review of audit logs as a preventive, detective and corrective controls

5. Database and system administration
    a. Roles and responsibilities of DBA and system administrator
    b. Process flow documentation
    c. Adequacy of controls to monitor activities of super users
    d. Menu options in different modules as per the 'Information Technology' policy of the bank

6. Application Security
    a. Review and report on adequacy of testing of security infrastructure at various stages of acquisition process

b. Undertake penetration tests of the information system
c. Secured Server Authentication procedures
d. General computer control's review like logical access to the internet banking application, OS, Database, Network and physical access control, Backup and program change management
e. Review and report on security controls

7. Networking
    a. Network Infrastructure Review, Network infrastructure at branch, Data Centre, DR site, offsite ATM and NAP (Network Aggregation Points)
    b. Network management and administrative review which includes Monitoring of structured cabling and network usage, optimization of setup, Bank with allocation (requirement/ utilization especially during peak hours for big/ service branches), corrective actions for the issues etc.
    c. Network Security

8. Capacity Management and Performance Tuning
    a. Determine Service Level Requirements for old servers
    b. Analyze current capacity
    c. Analyze network bandwidth availability at peak hours
    d. Planning for the future
    e. Analyze periodically workloads and services
    f. Measure overall resource usage
    g. Identification of unauthorized programs/ tools for removal

9. Organization – Wide Security
    a. Standard Operation Classification process that includes Documentation, Backup process, Storage of logs etc.
    b. Adequacy of anti-virus measures
    c. Adequacy of reporting
    d. Old information and device destroy procedures
    e. Firewalls, Network Intrusion Prevention Systems
    f. Architecture and placement of security devices etc.
    g. Security, ownership, source code, Documentation of Custom made application software

Evidence

Audit evidence should be sufficient, reliable, relevant, and useful in order for the auditor to form an opinion and to support their findings and conclusions. If the auditor cannot form an opinion based on the audit evidence obtained, the auditor should then obtain additional audit evidence. Procedures used to gather audit evidence varies depending on the information system being audited. The auditor should select the most appropriate procedure for the audit objective. The following procedures should be considered:

- Inquiry and/or Observation
- Inspection
- Re-performance
- Monitoring

The audit evidence gathered by the auditor should be documented and organized to support the auditor's findings and conclusions. Finally, when an auditor believes that sufficient audit evidence cannot be obtained, the auditor should disclose this fact as a limitation within the audit report.

Reporting

The audit report should be submitted to the Audit Committee through In-charge, Internal Audit Department. The IT auditor should provide a report in an appropriate form, upon the completion of the audit. The report should state the scope, objectives, period of coverage, and the nature, timing, and extent of the audit work performed. The report should state the findings, conclusions, and recommendations and any reservations, qualifications or limitations.