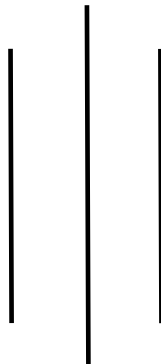


INTERNAL AUDIT POLICY 2075



(IA POLICY-2075)

Approved by:
706th Board Meeting
Held on 2075-05-20 (5th September, 2018)



NCC Bank
नेपाल क्रेडिट एण्ड कमर्स बैंक लि.
Nepal Credit & Commerce Bank Ltd.
Your Business Bank

The Board Meeting No. 706th
held on 2075.05.20 (5th September, 2018)
has decided to approved, the
"INTERNAL AUDIT POLICY-2075"

Kapil Gnawali
2075/09/28



Kapil Gnawali
Company secretary



Approval Sheet

Prepared By	Milan Rijal Officer, Internal Audit Department	
Reviewed By	Laxmi Prasad Duwal Head, Internal Audit Department	
Reviewed By	Ramesh Raj Aryal Chief Executive Officer	
Reviewed By	Audit Committee	
	Krishna Shrestha Coordinator	
	Madhav Prasad Bhatta Member	
	Kailash Patendra Amatya Director	
Reviewed By	Board of Directors	



Contents

1. Internal Audit Policy.....	1
2. Internal Audit	1
2.1 IAD positioning in overall Organization Chart.....	1
2.2 Defense line	1
3. Scope and Objectives.....	2
4. Strategies to achieve the Objectives.....	3
5. Core Values	4
6. Risk Focus.....	4
7. Authorities and Responsibilities	5
7.1 Board of Directors (BOD)	6
7.2 Audit Committee.....	6
7.3 Senior Management	6
7.4 Line Managers/Department Head/Branch Manager/Unit Head.....	7
7.5 Internal Audit Department	7
7.5.1 Authorities to Head IAD	7
7.5.2 Responsibilities of Head IAD	7
8. Independence and Conflict of Interests.....	8
9. Audit Manual.....	8
10. Information System (IS) Audit.....	9
11. Outsourcing of Audit.....	9
12. Coordination with Regulator and External Auditor	9
12.1 Coordination with Regulator.....	9
12.2 Coordination with External Auditors	10
13. Reporting.....	10
14. Applicability and Repeal.....	10
15. Review and Amendment.....	11
16. Disclaimer.....	11
❖ Annexure 1: Framework on Information System (IS) Audit.....	12

1. Internal Audit Policy

This Internal Audit Policy is to set out general principles under which Internal Audit function has to operate within Nepal Credit & Commerce (NCC) Bank Ltd. This policy shall act as a governance policy to be followed for all works undertaken by the Internal Audit Department (IAD).

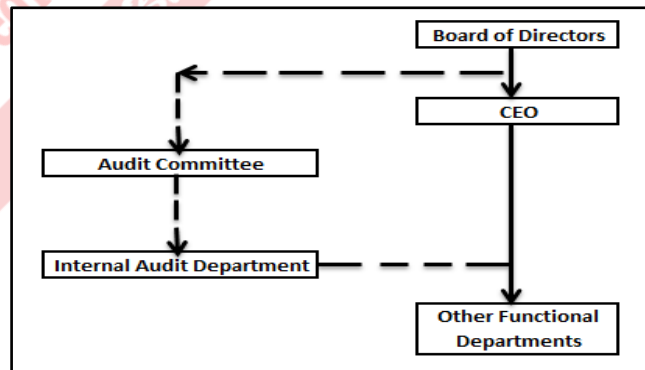
BASEL Accord issued by NRB has upheld the significance of Internal Audit function in banks. It has emphasized on efforts to harmonize and improve internal audit standards to align it with international standards. It has recognized internal audit as a part of the on-going monitoring of the bank's system 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. Internal Audit

As per the Institute of Internal Auditors (IIA), internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. Internal Audit shall remain a permanent, continuous and dynamic function in the Bank for which an internal audit department shall be constituted. It shall be an independent department that directly reports to Audit Committee of the Bank.

2.1 IAD positioning in overall Organization Chart

An independent Internal Audit Department (IAD) shall operate in the bank to conduct Internal Audit of the functions of the Bank. Activities of the IAD shall be supervised and reviewed directly by the Audit Committee and Board where necessary, in order to enable it to be independent. Head IAD shall also have dotted reporting line to CEO for only the administrative work of the department. Reporting line for IAD in the overall organizational chart shall be as per the structure presented alongside.



2.2 Defense line

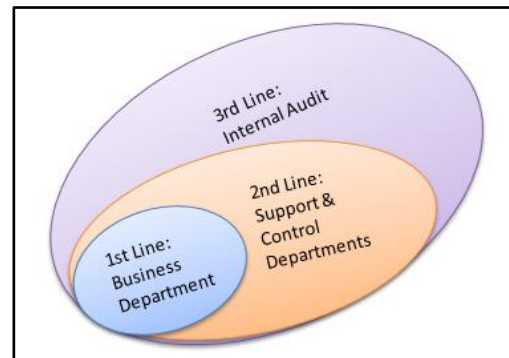
Relationship between IAD, business related departments and other support / control departments shall be linked by three line of defense model presented below.

a. First Line of Defense

Business related departments are the first line of defense since they undertake risks and are responsible primarily for identifying, assessing and controlling risks.

b. Second Line of Defense

Second line of defense comprises various support/control departments and senior management or executive having responsibilities of directing and supervising the entire affairs of the Bank.



They shall have secondary responsibility to identify, assess, monitor, mitigate and control risks since they are expected to work in close coordination with the business related departments.

c. Third Line of Defense

The third line of defense shall be the IAD that independently assesses the effectiveness and adequacy of risk management, internal controls and corporate governance designed in the first and second lines of defense and provides assurance on the same.

3. Scope and Objectives

The scope and objective of this policy shall be (but not limited to) as below:

SN	Scope Area	Internal Auditor's Objectives in relation to the Scope
1	Risk Management	Look into audit matters from perspective of various risks like Credit risk, Market Risk, Liquidity Risk, Operational Risk, Technology Risk, Staffing Risk, Strategic Risk, Financial Reporting Risk etc.
		Evaluation of risk appetite and decisions of risk management function.
		Assessment of risk management system regarding its ability to identify, measure, assess, control, respond to and report risks relating to the bank activities.
2	Capital Adequacy & Liquidity	Assessment of adequacy of Bank's Capital in relation to its risk exposures.
		Review the management's process of stress testing of Capital.
		Review the bank's systems and processes for measuring liquidity position.
3	Regulatory & Internal Reporting	Review accuracy, reliability and timeliness of reporting made to regulator and top management for decision making.
4	Compliance	Assessment of how effectively the compliance function is operating as a control function in the Bank.
		Review that Compliance function is effectively monitoring compliance to laws, regulations, internal policies etc.
5	Finance	Review and ensure appropriate application of applicable financial reporting framework.
		Assess whether the accounting controls in place are capable of identifying or detecting and correcting misstatements.
		See if necessary reconciliations are periodically done.
6	Internal Controls	Review and promote that there exist adequate internal controls in place for the prevention or timely detection and correction of misstatements.
		Enrich the bank with necessary recommendations to strengthen its controls in order to reduce chances of possible frauds.
7	Assets Safeguarding	Review the means of safeguarding Bank's assets.
8	Information system	Review whether Core Banking System (CBS) is capable of capturing all banking transactions on a timely manner.
		Review integrity of data and information generated from the Core Banking System (CBS) and test for data consistency.
		Implement the "Framework on Information System (IS) Audit" which is also an integral part of this policy under Annexure-1
9	Human Resource	Review HR Policy, its function and administration, HR Facilities and placement.
		Assess whether hiring and retention process of the Bank are adhered to.



SN	Scope Area	Internal Auditor's Objectives in relation to the Scope
		Assess other HR related issues like trainings, succession planning, appraisals, clearance during resignation, leave, attendances etc.
10	All Business and Support Departments	Review whether there exist any weaknesses or deviations from set procedures. Review whether there is the cost effectiveness and leakage of revenue. Recommend improvements or advice on best practices.
11	All Branches	Review the business operations of all the Branches as per approved annual audit plan, their processes and implementation of controls. Recommend improvements or advice on best practices.
12	Follow-ups	Review adherence to previous period audit recommendations. Review whether audit observations are properly addressed by audit units. Follow-up on implementation status of Regulator & External audits.
13	Certifications	Verify and certify periodic returns as per regulator's requirements.
14	Best Practices	Promote adoption of national/international best practices wherever practicable.
15	Other Special Functions	Conduct other special functions such as: a. Investigations - where fraud is suspected b. Surprise Audits - to test live operation of controls & processes c. Special Audits - on recommendation from top management / Board / Audit Committee.
16	Other functions in general	Play role of value provider rather than just a fault finder. Promote economy, efficiency and effectiveness of operations. Divert the audit focus from conventional to risk based approach. Divert more of its resources to areas considered material and risky. Review that the Bank is complying with all relevant laws, regulations, regulator's directions and internal policies and circulars. Ensure that the Bank is acting in the best interest of its stakeholders.

4. Strategies to achieve the Objectives

In order to attain the Internal Audit Objectives, following strategies shall be undertaken:

- Maintain independence and transparency during audit.
- Define the responsibilities of Board, Audit Committee, Senior Management, Head of Audit Unit, and Head IAD in regards to audit functions of the Bank.
- Maintain a preventive and proactive approach to audit rather than traditional detective and reactive approach.
- Standardize the internal audit function by developing an Internal Audit Manual.
- Develop an annual audit plan for the efficient and effective audit.
- Arrange necessary manpower for on-site and off-site audits.
- Empower the IAD with educated and experienced manpower.
- Promote IAD staffs for the update on different risks, regulatory requirements, internal policies, relevant acts by way of meetings for knowledge & problems sharing, workshops and trainings.
- Review business decisions made to ensure their consistency to the Bank's broad objectives.
- Review effectiveness of policies of the Bank and recommend improvements, where needed.
- Conduct audit with a risk-focus approach with professional skepticism and apply the principle of materiality during the audit.



- l. Conduct surprise visits and surprise audits to specified audit units and designated areas including audit of Bank/Branch's premises/properties after office hour.
- m. Conduct investigations / in-depth audit wherever fraud is suspected.
- n. Communicate to Audit Committee regarding the audit reports of audit units so that audit committee could directly send necessary instructions to Management and report to the Board.
- o. Coordinate with other Control Departments of the Bank to enhance the effectiveness of risk management, compliance, internal controls and corporate governance.
- p. Develop appropriate sampling techniques for the audits.
- q. Provide the audit unit with the opportunities for correction and defend before issuing Audit Reports.
- r. Any other procedures or techniques deemed necessary to achieve the internal audit objectives.

5. Core Values

Internal Audit Department, Head IAD and other staffs of the Department shall be guided by the following core values while discharging their professional responsibilities.

a. Integrity

Internal Auditors shall be honest, truthful and straight forward in discharging their professional responsibilities.

b. Objectivity

IAD shall maintain high standards of professional and independent Internal Audit Function and provide quality internal audit service in line with National/International best practices in the Banking sector. Internal auditors shall not allow any sort of bias or conflict of interest override their professional responsibilities. They shall not come under any undue influence while discharging their duties.

c. Professional Competence & Due Care

Internal Auditors shall have professional knowledge and skills at the level required to ensure that the Bank receives competent professional services. They shall work with due care and discharge their duties properly time.

d. Confidentiality

Auditors shall maintain confidentiality of information obtained by them while discharging their professional responsibilities and not use such information for their personal advantage or the advantage of any third party.

e. Professional Behavior

Internal Auditors shall present themselves on a professional manner while discharging their duties, comply with relevant laws and regulations, internal policies and circulars and avoid any actions that could discredit the Bank or the IAD itself.

f. Corporate Governance

It is the responsibility of Board of Directors (BOD) and Senior Management to maintain good corporate governance culture in the Bank. However Internal Auditor shall also carry out their functions with a view to add values in maintaining and promoting corporate governance culture in the Bank.

6. Risk Focus

Internal Audit Department shall switch focus from conventional compliance towards risk-based internal audit. IAD shall strive to add value to the Bank rather than just playing a role of fault finder. It shall

promote that a risk sensitive culture is incorporated into its activities. At the same time, the conventional roles of ensuring compliances and better controls shall also be performed.

IAD shall focus on inherent and control risks in business affairs of the Bank. Considering the level of these risks, IAD may undertake the detection risk and conduct its activities.

It may not be possible to conduct audit of all branches and departments on yearly basis and where audit is done, equal priority and resource of IAD may not be allocated in all areas of audit. Hence, there shall be allocation of more audit resources and its priority over relatively high risky areas and audit units for the optimum utilization of IAD resources and its effective result. For this, it shall require Risk Based Audit approach.

7. Authorities and Responsibilities

Bank is a highly regulated public limited company which is governed by Bank and Financial Institutions Act, Directives & Circulars issued by Nepal Rastra Bank, the Companies Act and other relevant laws of the nation. General responsibilities and functions of Audit Committee and IAD shall be guided by these Acts and provisions thereof.

Provisions laid down in BAFIA 2073, Companies Act 2063 & NRB Directives for the role of Audit Committee and provisions relating to conduction of Internal Audit in Banks and Financial Institutions are as below:

SN	Reference	Section / Clause	Provision
1	Companies Act 2063	164	<ul style="list-style-type: none"> Requirement of Audit Committee for a listed company with paid up capital of 30 Million or more.
		165	<ul style="list-style-type: none"> Functions, duties and powers of Audit Committee such as: <ul style="list-style-type: none"> Review internal controls & risk management Supervise and review Internal Auditing Perform other functions as per Board decision etc.
2	BAFIA 2073	60	<ul style="list-style-type: none"> Board shall form an Audit Committee.
		61	<ul style="list-style-type: none"> Functions, duties and powers of Audit Committee such as: <ul style="list-style-type: none"> Ensure proper internal controls & risk management Supervise and review Internal Auditing Provide information to Board for the matters of accounts, audit and internal control system.
3	NRB Directive No. 6, 2074	2 (KHA)	<ul style="list-style-type: none"> Board shall ensure regular Internal Audits IAD shall present its reports to Audit Committee at least quarterly
		7 (2)	<ul style="list-style-type: none"> Board shall form an Audit Committee under a non-executive Director. Internal Audit Committee shall: <ul style="list-style-type: none"> Review financial position / performance of Bank Discuss on operation of Internal Controls Prepare Internal Audit Manual Ensure conduction of Internal Audit as per Manual Review observations of Internal Audit Make necessary directions/advise to the Management Provide necessary advice to the Board etc.

These above provisions have made the Bank mandatory to constitute an Audit Committee and ensure an independent audit function within the Bank thereby instilling the provision regarding authorities of Board, Top Management, Audit Committee, Head IAD and other staffs of the Bank.

7.1 Board of Directors (BOD)

The Board, in the spirit of BAFIA 2073 [Section 60], shall form an Audit Committee where a non-executive Director shall be coordinator and Head IAD shall act as a member secretary. BOD shall ensure the independence of audit committee and IAD from the Business and other operational activities of the Bank. It shall review audit reports on periodic basis and accordingly instruct the management for the correction and implementation of audit comments /suggestions.

7.2 Audit Committee

The primary duties and responsibilities of Audit Committee shall be as per Companies Act 2063, BAFIA 2073 and the NRB Directives and circulars issued by NRB from time to time. It includes (but not limited to):

- To review the financial condition, internal control and risk management system of the Bank.
- To review the contents of the report of External Auditors and NRB Inspection, and it shall advise the management for the correction & implementation of the matters and recommendations therein.
- To review the financials of the Bank on quarterly basis and submit the report to the Board.
- To review the audit activities of the Branches and Departments that they are being performed as per "Annual Audit Plan".
- To ensure timely, efficient and effective audit functions are in place.
- To review the activities of the Bank as to whether they are economic, efficient, prudent, logical and effective and give necessary suggestions to the Board.
- To review the compliance issues reported by NRB, External Auditor and Internal Auditors. It shall instruct the Management for the rectification and report to the Board
- To perform other functions as stipulated in Companies Act 2063, BAFIA 2073 and NRB Directives.
- The meeting of committee shall be conducted as per the requirement of IAD/Bank.

In addition, the Committee shall perform any other functions as per the direction of the Board in regards to the Accounts, Internal Control System, Audit, Compliance and Inspection & Investigation.

7.3 Senior Management

The duties and responsibilities of senior management includes (but not limited to):

- To lead and be committed for correction / implementation of the audit issues and suggestions.
- To equip IAD with adequate manpower.
- To provide adequate resource and cooperation to Internal Audit Department.
- To strengthen first and second lines of defense of the Bank by devising appropriate control and monitoring systems.
- To give the opportunity of trainings and workshops for the IAD staffs.
- To boost the working culture of the Bank in such a way that every employee is encouraged and feels safe& self-respect in sharing suspicious transactions and fraud with competent authority.
- To promote the reward and punishment system that encourages performance with Compliance and discourages the breaches or resistances to Compliance.

7.4 Line Managers/Department Head/Branch Manager/Unit Head

Line Managers/Department Heads /Branch Managers /Unit Heads shall provide full cooperation and support to auditors during the course of the audit. S/he shall provide the documents, reports, audit reply and other details that auditors might ask for, during the course of the audit. In that case, s/he shall take the responsibility of correctness and accuracy on such matters.

S/he shall take the ownership of the auditor's report and show the commitment for the correction and implementation of the audit comment and suggestion. The repetition of frequent audit issues and being resistant for the correction shall be taken as a matter of non-compliance and the management shall take the appropriate action against them.

7.5 Internal Audit Department

The Bank shall constitute an independence internal audit department and Head IAD shall direct the activities of the Department for the attainment of objectives set out in this Policy with necessary strategies.

7.5.1 Authorities to Head IAD

Head IAD shall have following authorities:

- Unrestricted and unconditional access to all departments, offices, activities, records, information system, properties, personnel, etc. as deemed necessary and relevant for the purpose of conducting audit.
- To ask for adequate resources in IAD to accomplish its annual plan for the efficient & timely conduction of audit.
- Apply necessary audit procedures and techniques to accomplish the audit objectives.
- To inquire for explanations or ask for reports from any Department and Bank's officer(s) that might be required in the course of its regular, special and or investigation works.
- Other authorities as delegated by the Audit Committee or Board on case to case basis.
- Other authorities as per other laws of the nation and provisions therein.

7.5.2 Responsibilities of Head IAD

Head IAD shall be responsible for the entire affairs of IAD which includes:

- Work as the member secretary of Audit Committee.
- Demonstrate leadership and be an ambassador for Internal Audit function.
- Promote Good Governance throughout the organization.
- Provide consultancy services for organizational value addition.
- Develop a Manual and implement Risk based internal audit.
- Develop Annual Audit Plan and get it approved from the Audit Committee.
- Conduct internal audit and implement approved Annual Audit Plan.
- Provide necessary assistance to External Auditors and Regulators, when asked for.
- Ensure that there exists proper employee succession plan in the IAD.
- Monitor performance of IAD staffs.
- Ensure high standards of professional ethics and adherence to the Core Values in conduct of the IAD.
- Ensure that the IAD is updated for all changes in relevant laws and regulations, internal policies, regulator's directions and circulars.
- Leading and directing the internal audit service so that it makes a full contribution to and meets the needs of the Bank and its stakeholders.



- n. Present periodic status of audit and major weaknesses in internal controls and identified risks to the Audit Committee and Board.
- o. Conduct special audits and investigations, where fraud is suspected.
- p. Certify periodic returns as per requirements of the BAFIA / NRB Directives and ensure adherence to the provision of NRB and other laws relating to internal audit functions of the Bank.
- q. Any other responsibilities assigned by the Audit Committee or Board.

Head IAD may carry out the spot/specific audit or assignment as advised by the CEO, the Audit Committee, the Board of Directors or the Regulators. In that case, the authorities and responsibilities shall be as stipulated in such assignment. Further, Head IAD may also initiate such specific audit (if deemed necessary) with consent from the Audit Committee.

8. Independence and Conflict of Interests

All the staffs of IAD shall act with independence while executing their professional responsibilities and it shall be adhered to the core values. Independence comprises:

a. Independence of Mind

Audit officials shall stay in a position that their opinion will not be affected by any influences and they shall not compromise with their professional judgments.

b. Independence of Appearance

Audit officials shall not only remain independent, but shall also appear independent to all reasonable persons. They shall avoid any facts and circumstances and stay in a position where any third party cannot doubt on their independence. 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 IAD will not simultaneously be involved in other operational duties not compatible with Internal Audit Function. Sometimes, Head IAD or any other staffs of IAD may be assigned by the CEO and Other Senior Executives for the special tasks where the auditing expertise and investigating skills may be required. For assignment of Head IAD, consent of the Audit Committee shall be obtained and in case of other staffs of IAD, consent from the Head IAD shall be required for allowing them to involve in such special tasks not directly related to audit activities.


Auditors shall not have the line responsibility or authority over any of the operations they examine. This is to ensure the independence necessary for the Internal Auditors to exercise judgment, express opinions and present recommendations impartially.

- a. Head IAD shall be accountable and report to the Audit Committee.
- b. IAD will be independent of the activities of the audit unit. The department will also be independent from the internal control processes of the Bank.
- c. Internal Auditors shall exercise their assignment on their own initiative in all departments, offices and branches of the bank.
- d. Performance appraisal of Head IAD will be carried out by the members of Audit Committee whereas performance appraisal of other staffs of IAD shall be conducted by Head IAD and submit to Audit Committee for necessary review.

9. Audit Manual

This policy shall be supplemented by a separate Manual which shall further govern the activities of the IAD. The Manual shall act as an operational guide to the activities of IAD. The Manual shall be designed in the framework of Risk Based Internal Audit (RBIA). The objective of RBIA should be to prioritize

Handwritten signature and date:
2075/10/28



different areas of the audit universe based on risk levels and divert more audit resources to the riskier areas than areas considered comparatively less risky. RBIA Manual shall address matters such as:

- a. Rationale behind the RBIA Manual.
- b. Audit techniques.
- c. Modality for risk scoring and risk grading of audit units.
- d. Selection of audit units for audit.
- e. Assessment of IAD Resource.
- f. Audit plan and audit frequency.
- g. Audit program, procedures and its documentation in the implementation level.
- h. Any other matters deemed necessary to implement RBIA.

10. Information System (IS) Audit

In the recent era, Banking has become more complex and dependency over IS Environment. Accordingly, IS risks have also increased significantly with application of several IT application, architect, devices and gateways in the Banking system.

With this view, IT Guideline 2012 issued by NRB requires Banks to ensure sophisticated IS framework and its security system. It also requires Banks to ensure adequacy of IS security plan and control system that commensurate to the nature and business of the Bank. For this, the Bank shall also conduct IS Audit annually.

If the bank does not have technical and IS expert staffs in IAD to conduct IS Audit in a framework of annexure 1, IS audit can be outsourced from external professional service provider so as to comply with the NRB Guideline. Report of such IS audit shall be reviewed by Audit Committee and necessary instructions /suggestions shall be given to the management.

11. Outsourcing of Audit

In order to meet the human resource gap in IAD and the need of outsider expertise on case to case basis, the Bank may (if deemed necessary) consider outsourcing manpower to execute IAD activities after approval from the competent authority. Mode of Outsourcing may be:

- Outsourcing the audit staffs from auditing profession/firms for their independent audit in specific area(s), branch and department of the Bank and report to the Head IAD or Audit Committee.
- Outsourcing the technical expertise for non-recurring nature assignment.

Detailed cost benefit analysis, justification for the requirement of external expertise and internal resource gap analysis shall be prepared and approved by the Audit committee for any kind of outsourcing relating to activities of Internal Audit Department.

12. Coordination with Regulator and External Auditor

12.1 Coordination with Regulator

Nepal Rastra Bank (NRB) acts as the regulator of all banks and financial institutions (BFI's) in Nepal. Regulator keeps a close eye on the activities of licensed BFI's to:

- a. Assess the controls in place and its adequacy to prevent or detect and correct misstatements.
- b. Examine the risk management systems in place to identify, manage and minimize risks.
- c. Ensure whether good corporate governance practices are adhered to.
- d. Ensure that interest of depositors and other stakeholders are protected.

- e. Ensure that Regulator's directions and provision of laws/regulation of the country are followed.

Considering the above factors, objectives of IAD and the Regulator appear to coincide to a higher extent. Hence, regulators could rely on the work of IAD to some extent and may evaluate the objectivity, effectiveness, quality and independency of Internal Auditors. IAD shall ensure full cooperation to the external regulators for the matter they ask for. While providing any reports related to IAD to the regulator, the Bank shall duly inform Head IAD.

On the other hand, IAD is also expected to review that the regulator's comments and recommendations to the Bank through inspection and other special reports are duly complied with. Regulator may also provide feedbacks on ways to enhance efficiency and effectiveness of works of IAD. In that case, IAD shall duly implement the regulators suggestions.

12.2 Coordination with External Auditors

External audit of banks are made mandatory as per provisions of Companies Act and the Banks and Financial Institutions Act. External Auditors perform the audit of BFI's with the prime objective of expressing opinion as to whether the Financial Statements prepared by the BFI's give a true and fair view as per the applicable Financial Reporting Framework. External Auditors apply audit techniques and procedures to assess the internal control system, risk management system and integrity of the financial statement and ensures adherence to Nepal Standards on Auditing (NSA).

Therefore, the objective and nature of work of internal and external auditors also tend to coincide to some extent. Further, external auditors could be guided by **NSA 610** "Using the Work of Internal Auditors", so they might rely on the work of the internal auditors as well. Accordingly External auditors could request a copy of Internal Auditor's reports and wish to arrange a meeting with the IAD. In that case, IAD shall provide full assistance to the external auditors by providing copies of requested reports and responses to inquiries made by them.

On the other hand, Internal Auditors could also make use of reports of external auditors and conduct the follow up audit to review correction / implementation of External auditors' comments.

13. Reporting

In addition to statutory reporting and certification, Head IAD shall report directly to the Audit Committee of the Bank and forward a copy of the same to the CEO. S/he is required to cover the following aspects in the reports:

- Major remarks/observations of the internal audit reports on branches/ departments of the Bank, comments from the concerned audit units and recommendation of the IAD.
- Brief report on the investigations (if any) conducted by the Department.
- Review performance of the Bank.
- Significant lapses in control system, deviation from laid down policies and procedures of the Bank, implementation status of external audit report and NRB inspection report.
- The risks associated with the Bank business, operations and measures to mitigate the same.

Upon review of the internal auditor's report, the committee shall issue necessary suggestions/instructions to the management.

14. Applicability and Repeal

The Policy shall be applicable immediately upon approval by the Board and with that effect, previous Internal Audit Policy 2072 shall be repealed accordingly.

This policy is intended for the Bank's internal use only and remains the property of NCC Bank Limited. It shall be the responsibility of all staffs of the Bank to ensure that Policy and its contents are kept confidential at all times.

15. Review and Amendment

The Internal Audit Policy shall be refined and streamlined continuously to address the best practices in internal audit. The policy shall be subject to review annually and modification as per requirement considering national and international practices of auditing and to cope with the changes in internal and external policies and business environment.

16. Disclaimer

This internal audit policy has been prepared to make it consistent with BAFIA 2073, NRB Directives and circulars issued from time to time and Company Act 2063. In case any disputes/ contradictions arise in provisions of this policy and those contained in the NRB Directives/Companies Act /BAFIA, provisions in the latter shall prevail.



❖ **Annexure 1: Framework on Information System (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.

Information System Audit shall 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

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

2075/05/20



- 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.

Board of Directors:

S.N.	Name	Position	Signature
1.	Mr. Upendra Keshari Neupane	Chairman	
2.	Mr. Iman Singh Lama	Director	
3.	Mr. Chandra Prasad Bastola	Director	
4.	Mr. Madhav Prasad Bhatta	Director	
5.	Mr. Krishna Shrestha	Director	
6.	Dr. Kailash Patendra Amatya	Director	

