Compliance Unit

Operational Manual

National Rural and Renewable Energy Programme

Table of Contents

Abbreviation and Acronym 5

1. Background and Purpose 6

1.1. Introduction to NRREP 6

1.2. Principles governing the compliances 9

1.3. Purpose of Compliance Unit 11

1.4. Objectives of Compliance Unit 12

1.5. Functions of Compliance Unit 12

2. Administrative setup 13

2.1. Organizational design of compliance unit 13

2.2. Roles and responsibilities 14

2.3. Independence and Objectivity 15

2.4. Code of ethics and integrity 16

2.5. Governance framework 18

3. Compliance Review Methodology 23

3.1. Annual Audit Planning 24

3.2. Planning 27

3.3. Communication 34

3.4. Assessment and execution 37

3.5. Reporting 46

3.6. Documentation 49

3.7. Follow up 52

4. Compliance Reviews 53

4.1. Financial Review 55

4.2. Procurement Review 71

4.3. Performance review 74

4.4. Regulatory review 78

5. Management Information System 90

5.1. Purpose 90

5.2. Reporting requirements 90

5.3. MIS including action taken matrix 90

5.4. Formats 90

5.5. Risk universe database 91

6. Quality Assurance 94
6.1. Quality assurance framework 94
6.2. Policies and guidelines 95
6.3. Frequency and responsibility 95
6.4. Quality assurance assessment 96
6.5. Quality assurance methods 96
6.6. References 96
7. Capacity Development 97
7.1. Objective 97
7.2. Needs assessment 98
7.3. Planning 99
7.4. Capacity development program 100
7.4.1. Capacity development program for audit firms/ organizations on panel of Compliance Unit 100
7.4.2. Capacity development program for individuals 101
8. Annexes 105

Preface

The Alternative Energy Promotion Centre (AEPC) was established by Government of Nepal (GoN) on 3 November 1996, with the purpose of developing and promoting renewable energy technologies in Nepal. In 2011, the Government of Nepal and development partners jointly agreed to support formulation of a National Rural and Renewable Energy Programme (NRREP).

NRREP emphasizes on effectively reaching out to the remote and poorest parts of the country. It applies demand led approaches actively involving beneficiaries in decision making, and support use of energy for productive purposes leading to income and employment increase in rural areas and it has mainstreamed Gender and Social Inclusion (GESI) into the programme at all levels

The Compliance unit within NRREP is responsible for quality assurance of all financial management, planning and control systems of NRREP including CREF (Central Renewable Energy Fund) and to ensure compliance with the approved systems.

It will be the responsibility of the Compliance Unit, based upon their findings, to advise the relevant CREF unit as well as AEPC on how systems and procedures can be improved. The Compliance Unit will also provide a report stating overall findings of their assessments and quality assurance audits to the NRREP Programme Steering Committee through the lead development partner. The Unit is independent unit from NRREP Components and NRREP Programme Management Team.

Compliance unit is managed in the programme document and thus the Compliance Unit’s roles and responsibility shall also include an objective to reduce fiduciary risks and enhance efficiency and effectiveness of NRREP.

Abbreviation and Acronym

AEPC	:	Alternative Energy Promotion Centre
COSO	:	Committee Of Sponsoring Organization
CREF	:	Central Renewable Energy Fund
ESAP	:	Energy Sector Assistance Programme
GESI	:	Gender and Social Inclusion
GoN	:	Government Of Nepal
IIA	:	Institute Of Internal Auditors
M&E	:	Monitoring and Evaluation
MIS	:	Management Information System
MSME	:	Micro, Small and Medium Sized Enterprises
NCA	:	National Compliance Advisor
NRREP	:	National Rural and Renewable Energy Programme
OAG	:	Office of the Auditor General
ORCA	:	Objectives, Risks, Control and Alignment
PEU	:	Productive Energy Use
RCM	:	Risk Control Matrix
RE	:	Renewable Energy
RET	:	Renewable Energy Technologies
SCA	:	International Senior Compliance Advisor
SIAs	:	Standard Of Internal Audits

1. Background and Purpose

1.1. Introduction to NRREP

The Alternative Energy Promotion Centre (AEPC) was established by Government of Nepal (GoN) on 3 November 1996, with the purpose of developing and promoting renewable energy technologies in Nepal. AEPC has positioned itself as an established national focal point for the Renewable Energy sector development in Nepal. The AEPC has hosted different project interventions through support from development partners. In particular, the second phase of the Energy Sector Assistance Program (ESAP II), implemented by AEPC from 2007 to 2012, followed a coherent and coordinated approach, which led towards realization of the need for a more coordinated sector development approach. As a result of it, in 2011, the GoN and development partners jointly agreed to support formulation of a National Rural and Renewable Energy Programme (NRREP). NRREP follows single programme modality in which there are no other AEPC executed, development partner supported renewable energy programmes or projects outside NRREP. The structure of NRREP is depicted in the figure below:

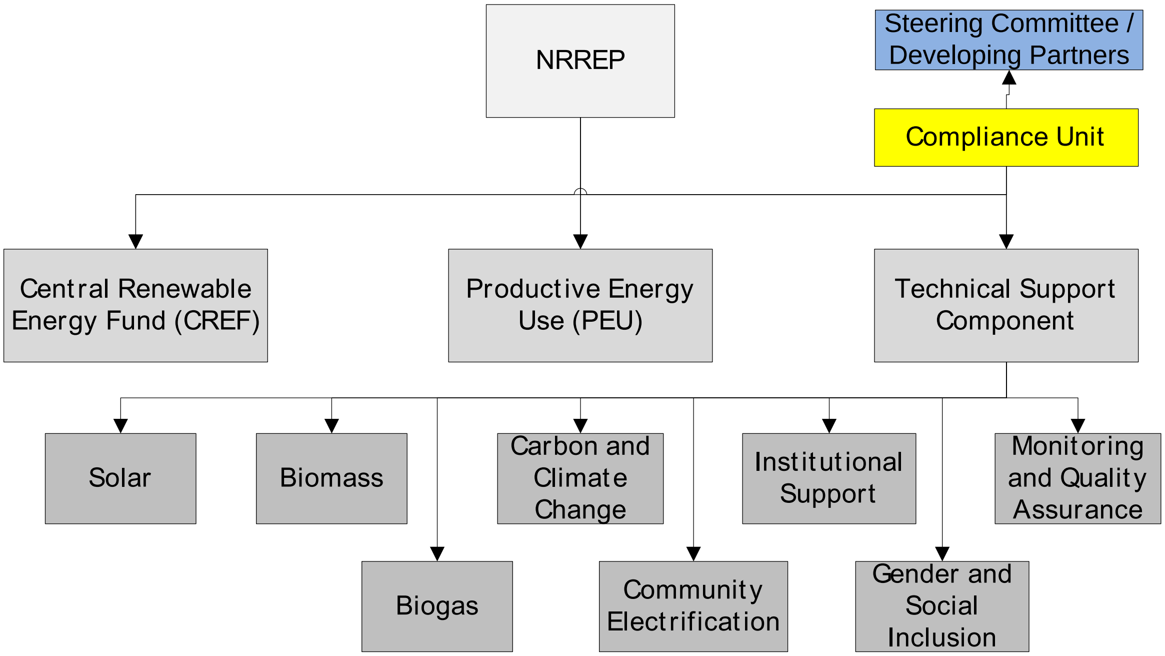

NRREP
Steering Committee / Developing Partners
Compliance Unit
Central Renewable Energy Fund (CREF)
Productive Energy Use (PEU)
Technical Support Component
Solar
Biomass
Carbon and Climate Change
Institutional Support
Monitoring and Quality Assurance
Biogas
Community Electrification
Gender and Social Inclusion

Figure 1: NRREP Structure

Objective

The development objective of the National Rural and Renewable Energy Programme (NRREP) is to:

- improve the living standard of rural women and men,
- increase employment/productivity of women and men,
- reduce dependency on traditional energy; and
- attain sustainable development through integration of alternative energy with the socioeconomic activities of women and men in rural communities.

NRREP emphasizes on effectively reaching out to the remote and poorest parts of the country. It applies demand led approaches actively involving beneficiaries in decision making, and support use of energy for productive purposes leading to income and employment increase in rural areas and it has mainstreamed Gender and Social Inclusion (GESI) into the programme at all levels.

GESI mainstreaming is done by including it in the development objective, each of the immediate objectives, in relevant outputs and activities, in indicators and targets as well as in monitoring. It is expected that the Government of Nepal (GoN) will mainstream GESI in the energy sector by providing equal access to and control of renewable energy technologies (RET) to increase contributions of rural women and men towards economic growth. This is in line with the GoN commitment to mainstream GESI and empowerment of women in the interim 3 year (2010-2013) plan.

Single programme modality

A distinctive feature of NRREP is that it is a single programme modality in which there are no other AEPC executed, Development Partner supported renewable energy programmes or projects funded outside the NRREP. This is made to remove inefficiencies, duplication, lack of co-ordination, supply led projects and fragmentation of aid to the rural and renewable energy sector in Nepal.

Program Components of NRREP

NRREP programme is divided into three components; first Central Renewable Energy Fund, second Productive Energy Use and third Technical Support Component. Each component has its own unique objective, implementation strategy and budget. The three components are structured to support each other towards attainment of common programme goal. Details of the three components are provided in the following section.

Component 1: Central renewable energy fund

The immediate objective of the Central Renewable Energy Fund (CREF) Component is to institute the CREF as the core financial institution responsible for the effective delivery of subsidies and credit support to the renewable energy sector.

This objective will be reached through establishing the CREF as an independently resourced and managed organization with the capacity to effectively deliver subsidies and credit financing support to help implement RET deployment at household and community levels.

Component 2: Productive Energy Use

The immediate objective of the Business Development for Renewable Energy and Productive Energy Use (PEU) Component is to contribute to an increase in income generation and employment potential for micro, small and medium sized enterprises (MSME) in rural areas, particularly for men and women belonging to socially and economically disadvantaged groups. This will be reached through three outputs:

(i) Capacities of existing MSMEs are enhanced;

(ii) New and innovative MSMEs are created and operationalised, with a specific emphasis on integrating women and marginalised section of the population, and

(iii) Appropriate Business Development Services are available to MSMEs in renewable energy catchments areas.

Component 3: Technical Support

The immediate objective of the Technical Support Component is to accelerate renewable energy service delivery with better quality, comprising various technologies, to remote rural households, enterprises and communities. Accelerated service delivery of renewable energy technology aims to benefit men and women from all social groups, leading to more equitable economic growth. Support for Several RETs, each with their distinctive characteristics, implementation strategies and institutional building support will be provided to AEPC and the decentralized structures.

Within biomass, better quality Improved Cooking Stoves will be delivered to an increasing number of rural households, in particular to the poor in remote districts. Focus will be on strengthening promotion of biogas in the household market and expanding promotion into the institutional market. Within the area of solar energy, lower cost domestic solar electric systems will be delivered more efficiently to an increasing number of rural households, and solar thermal applications will be promoted in a GESI and poverty relevant manner. The financial viability of community electrification schemes will be increased, and it will be sought to maximize availability of productive electricity at the village level. The strategy is to assist the AEPC, through implementation of its Strategic Organizational Development plan, to become an effective, efficient and GESI proactive institution for the promotion and development of the Renewable Energy (RE) sector.

One of the potential effects of the Technical Support Component will be a strengthened RET supply sector in Nepal. Through the use of the private RET sector, its capability will be increased to supply more and better quality RETs as well as potentially carry out innovation activities. With the substantial support provided to the various RETs and with the high number of beneficiaries of NRREP, this green economy sector will be stronger at the end of the five years NRREP implementation period. This provides opportunities for RET suppliers to have a foundation for increasingly supplying to the non-subsidized markets.

NRREP Management

The overall management of NRREP is carried out by the NRREP Programme Steering Committee. AEPC is the executing agency and Executive Director of AEPC acts as the NRREP Programme Director. Day-to-day management of the Technical Support and Business Development for Renewable Energy and Productive Energy Use Components is the responsibility of AEPC Programme Managers. The NRREP Programme Steering Committee has established the CREF Investment Committee with the overall responsibility of strategic management, planning and monitoring of CREF operations and performance. The Committee has established a Secretariat to support it at the operational level.

NRREP is a complex project which consists of various components and sub-components. Each component has its own objectives, budget and implementation modality. It is important to monitor the progress and take timely corrective actions in order to manage such extensive project efficiently and to achieve desired outcomes. Continuous assessment of project implementation in relation to established schedules and parameters is essential for effective monitoring. Monitoring will provide managers and other stakeholders with continuous feedback on implementation. Identify actual or potential successes and problems as early as possible to facilitate timely adjustments to programme implementation.

A Compliance Unit has been established to provide oversight and support to financial and procurement management as well as for quality assurance and support to Value for Money audits across NRREP. The Compliance unit is headed by a International Senior Compliance Adviser (ISCA), who is supported by a National Compliance Advisor (NCA).

1.2. Principles governing the compliances

The Institute of Internal Auditors (IIA) defines Internal Audit as:

“Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.”

The Institute of Chartered Accountants of India defines Internal Audit as:

“Internal audit is an independent management function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity’s strategic risk management and internal control system.”

The above definitions of internal audit call for internal audit, to be an independent function within an organisation placing greater emphasis on its objectivity. Thus internal auditing primarily provides an independent objective opinion to the Head of the Department/ Office.

The evolution of Internal Audit as described above may be depicted in the diagram below, showing maturity of Internal Audit in a modern organisation:

Transforming Internal Audit			
Internal Audit Maturity Model			
Philosophy			
Perspective	Focus on the past: retrospective look at what happened	Focus on the present	Focus on the future: proactive approach toward risk mitigation and development of controls

Transforming Internal Audit			
Internal Audit Maturity Model			
Defining Effectiveness			
Focus	Audit entity based on rotation plan	Audit entity prioritised based on inherent risk	Focus on strategic, organisational and process risk
Style	Policing	Supportive	Advisor
Organisational Structure			
Responsibility	Auditing for Compliance	Auditing and Suggesting	Auditing and Consulting
Existence of Chief Audit Executive (Director - Internal Audit)	Not Likely	Occasionally	Member of "C" Suite
Internal Audit Reporting Lines	Controller	Principal Secretary - Finance	Audit Committee
Independence and Objectivity	Hopefully	Generally	Absolutely
Technology			
IT Auditing	ill-defined	application controls	General Computer Control, Security and Application Controls
Fraud Detection			
Fraud prevention and detection	Generally not addressed	Reactive	Proactive
Risk Management			
Risk Focus	Operation	Operation and Financial	Enterprise Risk

This manual provides a framework for delivering consistent, high quality internal audit services. The framework and methodology suggested in this manual are aligned to International Standards for the Professional Practice of Internal Auditing (the "IIA Standards") and Standards on Internal Audits (SIAs) published by Institute of Chartered Accountants of India.

The IIA standards consist of Attribute and Performance Standards. Attribute standards address the attributes of organisations and individuals performing internal audits. Performance standards describe the nature of internal auditing and provide quality criteria against which the performance of these standards can be measured. In addition to the standards, practice advisories and practice notes/guides on current topics and trends in internal audit are released by the IIA on a periodic basis. This guidance is available on website www.theiia.org and must be referred for all reviews.

The NRREP Monitoring & Evaluation (M&E) system is aligned to GoN's monitoring requirements. The objective of the M&E system is to provide systematic feed back to NRREP management to enable adjustments to implementation strategies and outputs in order to effectively reach the expected outcomes and contribute to realization of the development objective. Monitoring in NRREP is a management tool that enables result-based management. At the development and immediate objective levels, where indicators and targets have been defined, the M&E system will regularly make assessments on the degree of progress towards reaching the development impact and outcome. A baseline has been produced in 2011, and covers all the RETs delivered through renewable energy programmes and projects. Focus will be on result based monitoring of energy related climate change impacts and socio-economic impacts.

The design of the NRREP M&E system benefits from and is done in conjunction with design of the system for monitoring of the Business Development for Renewable Energy and Productive Energy Use Component, which will be developed to be compliant with the "Donor Committee on Enterprise Development" standards on measuring and reporting results.

The objective of this manual is to support the Compliance Unit of NRREP to accomplish its objectives of internal audit function and capacity building. Traditionally, people understand internal audit as an activity of self imposed internal check and audit which also supposedly involved the activity of going around telling people what they were doing wrong. However even if one sees it in a narrow sense , the contribution of the activity of internal audit is potentially of major importance, as an effective internal audit system leads to improved accountability, ethical and professional practices, effective risk management, improves quality of output and supports decision making and performance tracking. An effective internal audit function can support the attainment of NRREP goals by providing timely information on deviations and recommendations of corrective actions.

1.3. Purpose of Compliance Unit

The Compliance unit within NRREP is responsible for quality assurance of all financial management, planning and control systems of NRREP including CREF and to ensure compliance with the approved systems. The Compliance Unit conducts random quality assurance/compliance audits.

The Compliance Unit advises CREF as well as AEPC on how systems and procedures can be improved. The Compliance Unit also provides a report stating overall findings of their assessments and quality assurance audits to the NRREP Programme Steering Committee through the lead development partner as well as to the CREF Investment Committee. The Compliance Unit works in close consultation with the Secretariat of the CREF Investment Committee. It is the responsibility of the CREF Investment Committee to follow-up on findings and recommendations made by the Compliance Unit.

The main purpose of Compliance Unit is to provide assurance and advisory concerning:

- Effectiveness of operations of internal control
- Effectiveness of risk management system
- Compliance with laws, rules and regulations
- Adequacy of accounting and record keeping
- Economy, efficiency and effectiveness of activities and operations
- Accountability and transparency in decision making process; and
- Special review and investigations

1.4. Objectives of Compliance Unit

Objectives of Compliance Unit are as follows:

- Provide oversight of financial and procurement activities, quality assurance support to all elements of NRREP.
- Capacity building support in Public Financial Management in AEPC and other public sector institutions receiving support from NRREP.
- Procurement of technical assistance.
- Conduct random quality assurance/compliance audits
- Advice on systems and procedures improvement.
- Mitigate fiduciary risks and enhance efficiency and effectiveness of NRREP

1.5. Functions of Compliance Unit

The functions of compliance unit are as follows:

- Prepare annual plan for monitoring and quality assurance by preparing a calendar for compliance reviews to be carried out during the year
- Prepare scope of work to hire external consultants to carry out the compliance reviews
- Shortlist and contract external consultants for compliance reviews
- Monitor the work of external consultants and review the reports submitted for compliance reviews conducted during the year
- Conduct random quality assurance/compliance audits in the CREF Handling Bank and in the Prequalified Partner Banks
- Regular reporting to steering committee of NRREP through lead donors on key findings of the compliance reviews
- Provide capacity building support to elements of NRREP by providing guidance in respect of financial management capacity by providing advise on improvement on the basis of compliance audit findings
- Follow up on audit findings and review the progress against action plan finalized in response to audit findings
- Report to steering committee on the progress against action plans
- Review of the NRREP's policies and procedures and their updates
- Ensuring familiarization of rules and regulations to employees and compliance professionals,
- Maintaining proper communication, internal monitoring, standard enforcements for NRREP.

2. Administrative setup

2.1. Organizational design of compliance unit

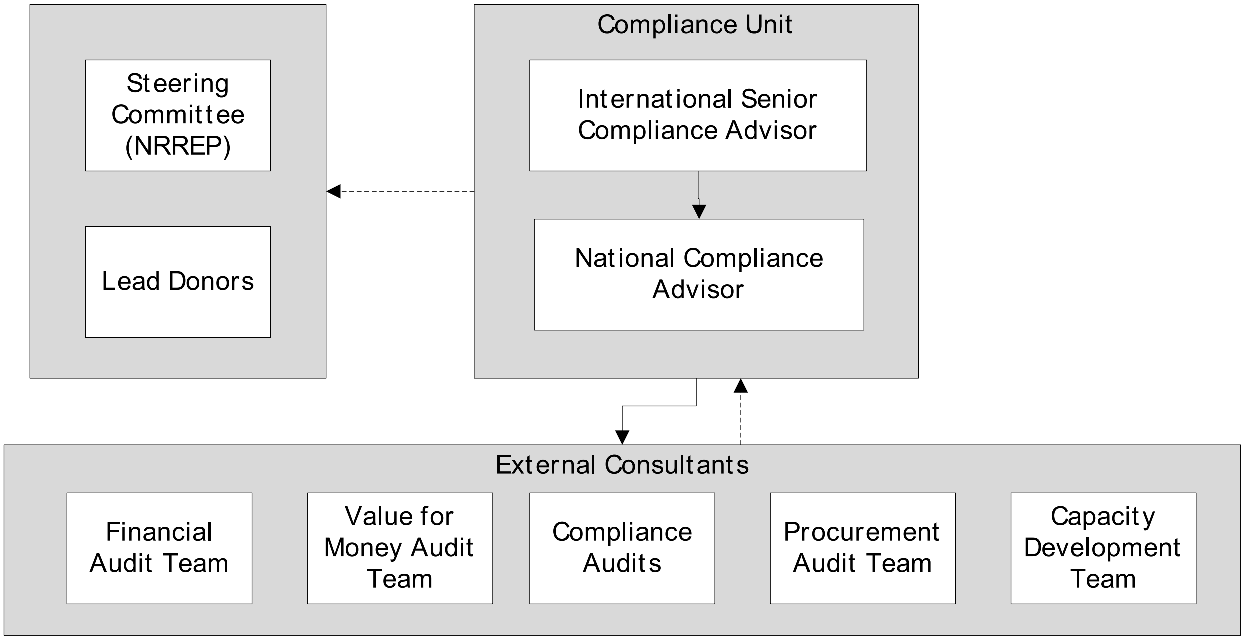

Steering Committee (NRREP)
Lead Donors
Compliance Unit
International Senior Compliance Advisor
National Compliance Advisor
External Consultants
Financial Audit Team
Value for Money Audit Team
Compliance Audits
Procurement Audit Team
Capacity Development Team

Figure 2: Organizational structure and reporting channels of compliance unit

The above figure represents the organizational structure of Compliance Unit and reporting channels in place. The reporting is represented by dotted lines. Compliance Unit is headed by an International Senior Compliance Advisor and supported by a National Compliance Advisor. Compliance Unit contracts external consultant to conduct financial, performance, procurement and regulatory audits. External consultants conduct field audits and report the findings to Compliance Unit. Compliance Unit is responsible for quality assurance of audits conducted by external consultants and to report the findings and corrective action plan to Steering Committee of NRREP through lead donors.

Mission

"The compliance unit would ethically drive components across National Rural and Renewable Energy Programme by creating value to stakeholders in the socio-economic context through competencies drawn from the integration of strategy, management and accounting."

Vision

"The compliance unit would be the leading centre for excellence in the Sector as per the international best practices and source of professionalism for replication in similar setups across Government of Nepal's offices."

2.2. Roles and responsibilities

Compliance unit is headed by an International Senior Compliance Advisor (ISCA). The ISCA is responsible to NRREP Programme Steering Committee through the lead development partner. The main tasks of the ISCA is to manage the NRREP Compliance unit, which is responsible for compliance of all financial management, planning, control systems and approved systems of NRREP. The detailed functions include, but are not limited to:

- Prepare a schedule for and the scope of regular compliance audits as well as procurement audits for the approval by the NRREP Programme Steering Committee;
- Develop terms of reference to select and manage external contractors for regular compliance audits in accordance with approved schedule;
- Provide regular reports to the NRREP Programme Steering Committee on programme quality assurance systems and procedures as well as compliance with approved systems;
- Make recommendations to the NRREP Programme Steering Committee for improvements in financial management, planning and control systems including procurements within AEPC and CREF as the executing and implementing agencies;
- Support CREF in the design and implementation of financial management and control systems including guiding the establishment and operationalization of the CREF Internal Audit function, and offer general management advice to the CREF Board
- Provide advice and support to all elements of NRREP financial management, planning and control systems including procurement procedures and assess compliance to established systems and procedures;
- Support financial management functions of NRREP including preparation of budgets, accounting, financial reporting and auditing;
- Provide capacity development support in financial management to staff of AEPC, CREF and other institutions as needed and relevant;
- Facilitate that all approved work plans and budgets, progress and all audit reports are posted on the internet;
- Support preparation by AEPC of regular price analysis for renewable energy technologies;
- Provide support to the monitoring and quality assurance functions of AEPC and CREF as supported by NRREP;
- Provide support to review missions as well as to the external auditors as required;
- Support preparation and updating of NRREP Financial Management and Procurement Manuals;
- Review and endorse requests to Development Partners for transfer of funds to NRREP; and
- Plan and supervise the work of the national NRREP National Compliance Adviser to the International Senior Compliance Adviser as well as other staff assigned to the Compliance unit

International Senior Compliance Advisor together with National Compliance Advisor (NCA) is posted at AEPC and head the compliance unit. Various audits are conducted by external consultants selected as per the terms of reference prepared by ISCA and NCA. This operational manual serves as a guide to conduct the audits as per the requirements of NRREP.

2.3. Independence and Objectivity

The internal audit activity must be independent, and internal auditors should be objective in performing their work.

Organizational Independence

The International Senior Compliance Advisor must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The International Senior Compliance Advisor must confirm to the Steering Committee, at least annually, the organizational independence of the internal audit activity.

- The internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results.
- The ISCA must communicate and interact directly with the Steering Committee.
- Internal auditors must have an impartial, unbiased attitude and avoid conflicts of interest.
- If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.
- Internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an internal auditor provides assurance services for an activity for which the internal auditor had responsibility within the previous year.
- If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure must be made to the ISCA prior to accepting the engagement.

Individual Independence and objectivity

Auditors should have an impartial, unbiased attitude, characterized by integrity and an objective approach to work, and should avoid conflicts of interest. They should not allow external factors to compromise their professional judgment. Objectivity is an independent mental attitude that means honesty, freedom from bias, using facts without distortions from personal feelings or prejudices. Auditors should display appropriate professional objectivity when providing their opinions, assessments and recommendations. In assigning staff to audits, NRREP requires that the staff members are free of any restrictions to their independence and objectivity in performing the audits. To this end, internal audit staff:

- Shall not be placed in situations in which they feel unable to make objective professional judgments
- Shall not be assigned to audits where any perceived or actual conflicts of interest and bias are present

- Shall report to the ISCA any situations in which a conflict of interest or bias is present or may reasonably be inferred.

2.4. Code of ethics and integrity

Code of ethics

The Code of Ethics relevant for the Compliance Unit as its primary function is to act as an internal audit unit within NRREP. The principles governing the conduct of Internal Auditors are Integrity, Objectivity, Competency, Confidentiality and Independence.

Integrity

The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment. To exhibit Integrity Internal auditors:

- Shall perform their work with honesty, diligence, and responsibility.
- Shall observe the law and make disclosures expected by the law and the profession.
- Shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the profession of internal auditing or to the organization.
- Shall respect and contribute to the legitimate and ethical objectives of the organization.

Objectivity

Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgments. To exhibit objectivity in conducting internal audit, the auditors:

- Shall not participate in any activity or relationship that may impair or be presumed to impair their unbiased assessment. This participation includes those activities or relationships that may be in conflict with the interests of the organization.
- Shall not accept anything that may impair or be presumed to impair their professional judgment.
- Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.

Confidentiality

Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so. It is recommended that to maintain confidentiality the auditors:

- Shall be prudent in the use and protection of information acquired in the course of their duties.
- Shall not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization.

Competency

Internal auditors apply the knowledge, skills, and experience needed in the performance of internal audit services. It is recommended that internal auditors:

- Shall engage only in those services for which they have the necessary knowledge, skills, and experience.
- Shall perform internal audit services in accordance with the International Standards for the Professional Practice of Internal Auditing.
- Shall continually improve their proficiency and the effectiveness and quality of their services.

Professional Standards

The international standards promulgated by Institute of Internal Auditors for the professional practice of Internal Auditing are to be referred as guidance while conducting internal audit. Applicable standards are divided into 'Attribute Standards' and 'Performance Standards'. The list of standards is as follows:

Attribute Standards	Performance Standards
1000 – Purpose, Authority, and Responsibility	2000 – Managing the Internal Audit Activity
1010 – Recognition of the Definition of Internal Auditing, the Code of Ethics, and the Standards in the Internal Audit Charter	2010 – Planning
1100 – Independence and Objectivity	2020 – Communication and Approval
1110 – Organizational Independence	2030 – Resource Management
1111 – Direct Interaction with the Board	2040 – Policies and Procedures
1120 – Individual Objectivity	2050 – Coordination
1130 – Impairments to Independence or Objectivity	2060 – Reporting to Senior Management and the Board
1200 – Proficiency and Due Professional Care	2070 - External Service Provider and Organizational Responsibility for Internal Auditing
1210 – Proficiency	2100 – Nature of Work
1220 – Due Professional Care	2110 – Governance
1230 – Continuing Professional Development	2120 – Risk Management
1300 – Quality Assurance and Improvement Program	2130 – Control
1310 – Requirements of the Quality Assurance and Improvement Program	2200 – Engagement Planning
1311 – Internal Assessments	2201 – Planning Considerations
1312 – External Assessments	2210 – Engagement Objectives

Attribute Standards	Performance Standards
1320 – Reporting on the Quality Assurance and Improvement Program	2220 – Engagement Scope
1321 – Use of "Conforms with the International Standards for the Professional Practice of Internal Auditing"	2230 – Engagement Resource Allocation
1322 – Disclosure of Nonconformance	2240 – Engagement Work Program
	2300 – Performing the Engagement 2310 – Identifying Information 2320 – Analysis and Evaluation 2330 – Documenting Information 2340 – Engagement Supervision 2400 – Communicating Results 2410 – Criteria for Communicating 2420 – Quality of Communications 2421 – Errors and Omissions 2430 – Use of "Conducted in Conformance with the International Standards for the Professional Practice of Internal Auditing"
	2431 - Engagement Disclosure of Nonconformance 2440 – Disseminating Results 2450 – Overall Opinions 2500 – Monitoring Progress 2600 – Resolution of Senior Management's Acceptance of Risks

Compliance and regulatory guidelines

Relevant compliance and regulatory guidelines to be followed for NRREP comprise of prevalent laws of Nepal relevant to AEPC, NRREP administrative and financial guidelines and implementation guidelines for each component/ sub-component. Before, commencement of internal audit, relevant laws and guidelines must be discussed and a comprehensive list must be prepared. All relevant guidelines must be collated before commencement of audit.

2.5. Governance framework

Reporting structure

Reporting structure of Compliance Unit is as follows:

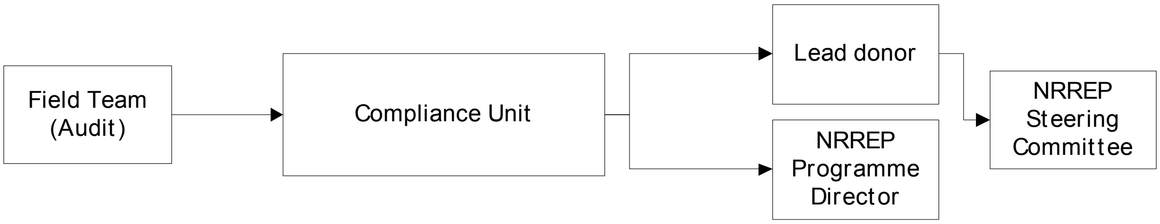


Figure 3: Reporting structure of Compliance Unit

The reporting structure of Compliance Unit is as per the above figure. As per the reporting requirements, the audit team in the field is required to report the audit findings and observations to the Audit team lead. The audit team lead shall review the audit observations and confirm the same with auditee and finalize and action plan.

Audit team lead is required to report the audit observations and action plan to National compliance advisor. Audit team lead shall report to NCA at the end of audit period through an audit report. Audit team lead shall report any cases of fraud/ mismanagement of funds to NCA immediately and discuss the further course of action. Further course of action may involve extending the scope of checking/ sample size of testing.

National Compliance Advisor shall consolidate the audit findings and report the audit findings together with progress report of ongoing audits to International Senior Compliance Advisor on monthly basis. ISCA as the head of Compliance Unit needs to report to Steering committee of NRREP through the lead donors. ISCA must report key audit findings of internal audit, progress of audits, quality assurance reviews, key performance statistics of compliance unit (as per chapter 7 of this manual) and action taken on audit observations. ISCA must present such reports in the quarterly meeting of Steering committee. A consolidated report on the audits conducted during the year shall be submitted to Steering committee at the end of each year.

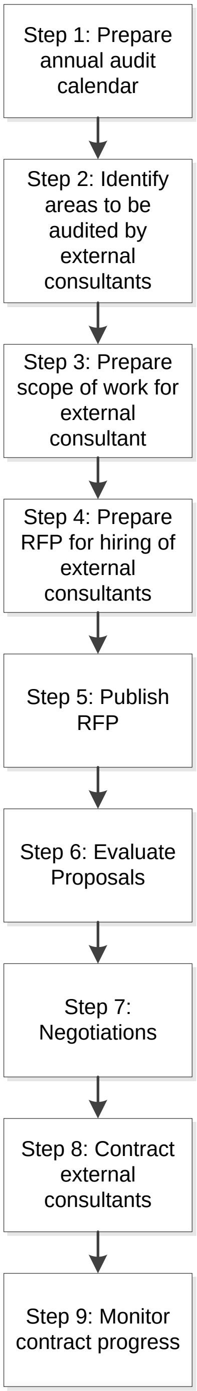
A summary of reporting arrangement is provided in the table below:

Reporting by	Reporting to	Key reporting parameters	Reporting frequency
Field team (Audit)	Audit team lead	Audit observations and findings	Regularly during the audits
Audit team lead	National Compliance Advisor	Audit observations, findings and action plan	At the end of audits, as per the terms of reference, as and when required for exceptional items i.e. mismanagement of funds, potential of collusion/ fraud
National Compliance Advisor	International Senior Compliance Advisor	Key audit findings, progress of ongoing audits	Monthly
International Senior Compliance Advisor	Lead Donor/ NRREP steering committee	Key audit findings, progress of audits	Quarterly during the year, consolidated

Reporting by	Reporting to	Key reporting parameters	Reporting frequency
		against the yearly audit calendar, quality assurance reviews, action taken on audit observations, MIS of compliance unit	report on yearly basis

External arrangements for conducting compliance reviews

Compliance reviews are conducted by external consultants contracted from time to time as per the annual audit calendar prepared by Compliance Unit at the beginning of each year. Refer Annexure – I for illustrative yearly audit calendar. Compliance reviews are monitored and reviewed by Compliance unit on regular basis. Steps involved in hiring of external consultants for compliance reviews are as follows:


Step 1: Prepare annual audit calendar
Step 2: Identify areas to be audited by external consultants
Step 3: Prepare scope of work for external consultant
Step 4: Prepare RFP for hiring of external consultants
Step 5: Publish RFP
Step 6: Evaluate Proposals
Step 7: Negotiations
Step 8: Contract external consultants
Step 9: Monitor contract progress

Step 1: Prepare annual audit calendar

An audit calendar lists the audits that will be carried out during the year. Audit calendar will have number of audits and audit entities to be audited under each category of audit (Financial, Performance, Procurement and Regulatory) during the financial year. Annual audit calendar needs to be prepared and approved at the beginning for each year. Audit calendar is prepared by the Compliance unit at the beginning of year and submitted to Steering committee in the first meeting of Steering committee in the beginning of financial year.

Step 2: Identify areas to be audited by external consultants

Total number of external consultants required to conduct audits must be identified on the basis of approved audit calendar. Man days must be estimated for each audit to calculate the input required for each audit. Total man days required for all audits during the year shall form the basis for number of external consultants to be hired during the year.

Step 3: Prepare scope of work for external consultants

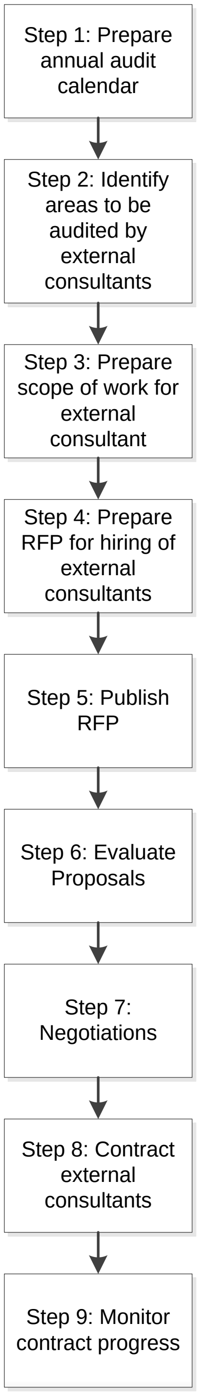
Scope of work for external consultants is prepared by the ISCA on the basis of nature of audits to be conducted during the year. Scope of work shall be detailed and precise to capture the work to be performed by the external consultant as per this operational manual.

Step 4: Prepare Request for Proposal (RFP) for hiring of external consultants

A Request for Proposal (RFP) shall be prepared to hire the external consultants. RFP must lay down the general rules for contracting as well as the scope of work prepared to hire the external consultants.

Step 5: Publish RFP

RFP shall be published in leading national newspapers and also published on the website of AEPC/ NRREP.


Step 1: Prepare annual audit calendar
Step 2: Identify areas to be audited by external consultants
Step 3: Prepare scope of work for external consultant
Step 4: Prepare RFP for hiring of external consultants
Step 5: Publish RFP
Step 6: Evaluate Proposals
Step 7: Negotiations
Step 8: Contract external consultants
Step 9: Monitor contract progress

Step 6: Evaluate proposals

Technical and financial proposals received from the external consultants shall be evaluated by the compliance unit. Hiring of consultants shall be done as per the administrative and financial guidelines of NRREP and Public Procurement Act/ Rules of Government of Nepal.

Step 7: Negotiations

Shortlisted consultants shall be called to negotiate on the financial proposals submitted by shortlisted consultants.

Step 8: Contract external consultants

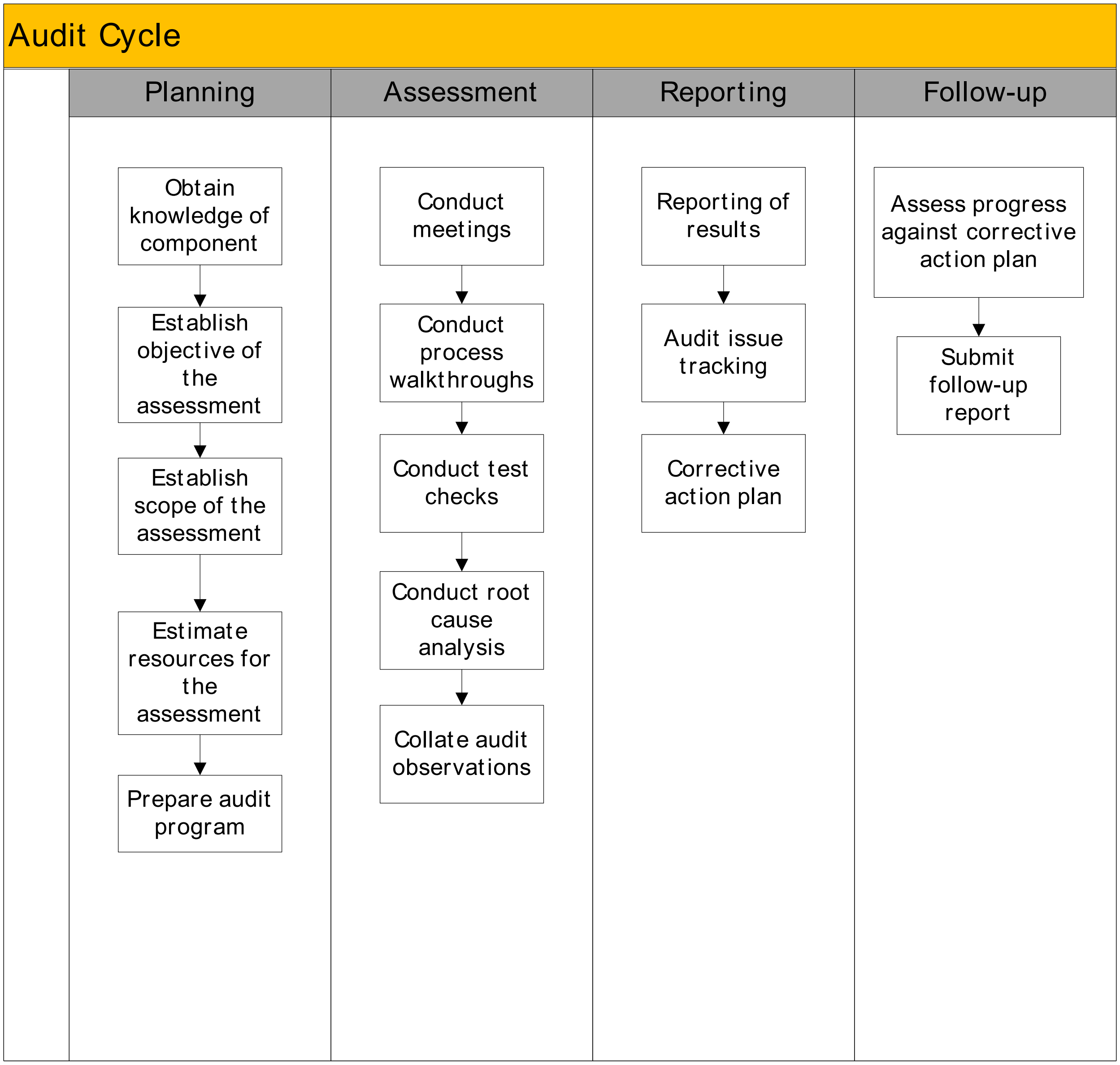
Consultants selected on the basis of evaluation of proposals and negotiations shall be contracted as per the standard contracting arrangements of NRREP.

Step 9: Monitor contract progress

Compliance unit is required to monitor the progress of external consultants as per the RFP and proposals submitted by the consultants. Any deviations must be discussed with the external consultants and addressed at the earliest possible.

3. Compliance Review Methodology

The compliance review process is comprised of four main stages: planning, assessment, reporting, and follow-up. Each stage is discussed in detail in this chapter. Compliance framework also recognizes that effective communication is essential to the success of compliance review and therefore is an important element embedded in each stage of the compliance review.


Audit Cycle
Planning
Assessment
Reporting
Follow-up
Obtain knowledge of component
Establish objective of the assessment
Establish scope of the assessment
Estimate resources for the assessment
Prepare audit program
Conduct meetings
Conduct process walkthroughs
Conduct test checks
Conduct root cause analysis
Collate audit observations
Reporting of results
Audit issue tracking
Corrective action plan
Assess progress against corrective action plan
Submit follow-up report

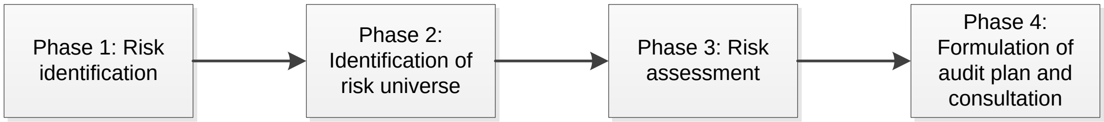
3.1. Annual Audit Planning

NRREP Internal audit plan objectives and process employed

The objectives of NRREP's Annual Risk-Based Internal Audit Plan are to:

- identify the priorities of Internal Audit, consistent with the objectives of NRREP;
- identify the priorities of Internal Audit based on an assessment of risk and potential exposure that may affect the NRREP's ability to accomplish its objectives;
- set out the audit universe for NRREP and timeframe needed for the provision of the annual holistic opinion on risk management, control and governance processes;
- share and coordinate activities with other internal and external providers of relevant compliance/ monitoring services to ensure proper coverage and minimize duplication of efforts;
- present Internal Audit's plans and resource requirements to the NRREP steering committee for review and approval respectively; and
- provide measures of success to previous year's internal audit activities.

The annual audit planning methodology has four main phases, each of which is described below.


Phase 1: Risk identification
Phase 2: Identification of risk universe
Phase 3: Risk assessment
Phase 4: Formulation of audit plan and consultation

Phase one: Risk identification

A series of interviews with NRREP Programme Director and component heads of NRREP are conducted between 15 June and 30 June (on rolling basis) every year with a view to identify risk profile to which NRREP operations are exposed. This risk information not only provides important insight into the concerns of management, but also provides risk exposure data which is used, as part of Phase Three, to prioritize and rank potential audit projects. Ultimately it leads to the ongoing reaffirmation of NRREP's audit universe and revisions to audit priorities.

Phase two: Identification of risk universe

The audit universe defines the potential scope of an organization's internal audit activity by segmenting its operations into individual "audit entities" that may be subjected to audit. Using the information provided by senior management in Phase One, the audit entities shall be identified and categorized according to the function they serve within NRREP. The audit universe is designed to reflect NRREP's key functions, as opposed to its structures in order to ensure the key risks to the achievement of NRREP's objectives are addressed.

As a result, the individual technical component, implementing agencies or entities that make up NRREP's structure are not directly identified as auditable entities. In recognition of the importance and materiality associated with them, Internal Audit will ensure that audit activities take place in all technical components, implementing agencies and entities over the three-year audit planning horizon. This will be done through the inclusion of a sample of technical components, implementing agencies and other entities for each audit undertaken based on the degree of risk posed and the necessity to reflect regional and technical differences.

For selection of entities for inclusion in NRREP's audit universe, three main criteria shall be applied. First, the entities must be auditable, i.e., they must be definable and have discrete objectives. Second, the entities must be significant and material in the context of the organization. Third, the entities must be relevant to NRREP's broader context. To summarise, each entity must relate to, and support, the achievement of NRREP's objectives.

Each entity must be classified on the risk scale of ‘High’, ‘Medium’ and ‘Low’. Relevant factors that must be considered in order to classify the entities on the risk scale could be change in management/ key staff or organizational structure, quantum of procurement, unusual variation in fiscal activities, high debt-capital ratio, unusually high transactions in cash etc.

Phase three: Risk assessment

In the first week of July, a full day workshop shall be conducted with NRREP programme director and technical component heads to rank each audit entity that makes up NRREP’s audit universe using the following three criteria, each of which is weighted to reflect its relative importance:

Risk Exposure of the Audit Entity: Using the risks identified in phase one, specific risks to each audit entity are identified and an aggregate risk score is developed. This criterion shall be assigned a weight of 50%.

*Significance of the Audit Enti*ty**:** Each audit entity is then assessed in terms of its significance which considered both overall importance of the entity to NRREP and the materiality associated with it. This criterion shall be assigned a weight of 30%.

Public Profile of the Audit Entity: Finally, the entity's public profile is examined and rated. This criterion shall be assigned a weight of 20%.

Taken together, these criteria shall be applied to derive a total weighted priority score which is used to generate a management assessment of the likelihood and impact of risks facing the NRREP.

A number of other risk determinants are used to identify the final risk rating and audit priority assigned to each of the entities. These comprise:

- changes to the materiality or monetary value of each audit entity;
- time lapsed since the audit entity was last audited and the results of recent audits (both internal audits and those completed by the OAG, Nepal) and monitoring activities;
- the frequency and results of evaluation reports; and
- senior management's most recent assessment of the viability of the audit universe and each audit element's risk rating.
- Change of management and/ or key staff

While identifying and populating risks, the fundamental assumption to be applied shall be the risks will not be eliminated - rather they will be managed and mitigated to bring them down to acceptable levels as per the risk appetite of the entity and Programme.
Consequently, risks shall be populated at a “Gross Level” to ensure that all the potential risks, irrespective of the existing controls and mitigating factors, are populated initially at the first level.
Subsequent to above, the risks shall be assessed, ranked and populated according to the likelihood and impact of them occurring to arrive at ‘residual level’.

For each risk, an impact may be assigned as either **high, medium or low** based on the following criteria:

High	Significant impact on XXX’s mission and/or strategy and/or objectives.
Medium	Moderate impact on the organization’s strategy or operational activities.
Low	Low impact on the organization’s strategy or operational activities.

An *indicative matrix* of guiding factors which may be used to assign the impact are provided below:

Risk Categories
Financial - Budgeting and Cash flow forecasting - Financial reporting
Operational (ability to manage people, processes & technology)
Reputation
Regulatory
Compliance framework
Environmental
Employees, Payroll Controls
Auditing

After assigning an impact to the gross risks and while assigning the likelihood/probability of occurrence, the existing controls and the steps already taken to mitigate such risks shall be considered to arrive at residual or net risks.

For each risk, its likelihood of occurrence may be assigned a probability of either **high**, **medium** or **low** based on the following criteria:

High (probable)	Potential of occurring several times in a time horizon of 1-3 years*
Medium (possible)	Possibility of occurring once in time horizon of 2-5 years*
Low (remote)	Has not occurred or is unlikely to occur in 4-10 years*

** Indicative time horizon (to be modified and updated on actual scenario and / or rolling basis)*

Final Risk Classification is therefore, at the **“Residual Risk”** level which takes into account the mitigating controls already in existence.

Audit planning shall place emphasis on risks and entities which were found to be under-controlled. These actions plans are in the nature of additional controls/actions required where the existing controls were found to be inadequate. A risk which has adequate mitigating controls in place would be assigned a low probability of occurrence and where adequate controls have not been established, the likelihood of occurrence could be medium/high depending upon the results of the walk through testing of transactions, that shall be planned to be carried out during audit execution. *Based on these testing results, the risk assessment matrix developed in the first year for the audit entities’ universe shall be updated on rolling basis*.

Phase Four: Formulation of the Audit Plan and Consultation

Taking into consideration the audit universe and risk rankings, audit projects are defined and plotted on a three-year planning cycle to reflect the following planning decisions:

- all high and medium ranked audit entities would be audited at least once on a three-year audit cycle;
- higher risk audit entities would be audited more frequently than three years some of which may have continuous audits scheduled in intervening years;
- low risk audit entities would not be audited but would be continued to be assessed for higher risk and hence the necessity for audit;
- each year would represent a body of work that could be reasonably achieved by the current complement of audit resources;
- mandated audits would be scheduled on a priority-basis;
- the management action plans derived from the observations and recommendations made in audits would be followed-up by Internal Audit within a reasonable period of time, usually one year, to determine the degree to which the management actions plans have been implemented;
- each year an allocation would be made to take into account donor directed audit work as well as management directed audits;
- the timing of audit projects would take into account program evaluations or OAG audits so as not to place an unreasonable burden on any one audit entity / responsibility centre or risk duplication of effort; and finally
- the overall plan would ensure sufficient coverage of NRREP's risk management, control and governance processes on an annual basis to collectively support the Senior International Compliance Advisor's holistic opinion.

An illustrative annual audit plan is provided in Annex – I.

3.2. Planning

At the beginning of each compliance review, the compliance unit together with audit team should, develop and document a plan for each review engagement to conduct the engagement in an efficient and timely manner. The audit working papers should have a documented audit plan for the engagement, setting out the objectives and scope of the audit and the techniques and resources to be used by the auditor.

Internal Audit Planning process suggested in this framework assumes four salient features:

a. Ownership of internal audit vests with the concerned auditee, represented by an 'owner' of the audit process

b. Internal Audit will perform Risk Based Internal Auditing

c. Internal Audit will have 3 layered approach plan to obtain maximum coverage :

   – Defined plan based on risk assessment

   – Surprise Audits based on analytics

   – Review of control self-assessment and compliance to be submitted by auditee

d. There should be an identified focal officer within compliance unit to provide the administrative support to the field teams and monitor the execution of the audit plan.

Internal audit plan should among other areas cover the following:

- Obtaining the knowledge of the legal and regulatory framework within which the auditee entity operates
- Obtaining the knowledge of the auditee's operations, accounting and internal control systems and policies
- Determining the effectiveness of the internal control procedures adopted by the auditee
- Determining the nature, timing and extent of procedures to be performed
- Identifying the activities warranting special focus based on the materiality and criticality of such activities, and their overall effect on operations of the department
- Identifying and allocating staff to the different activities to be undertaken
- Setting the time budget for each of the activities
- Expected completion dates for each of the activities
- Identifying the reporting responsibilities
- Communication plan during the course of audit

Planning may be revised as may be deemed necessary in the course of the audit in the light of newer findings or situations.

Planning Process

The planning process involves the following steps:

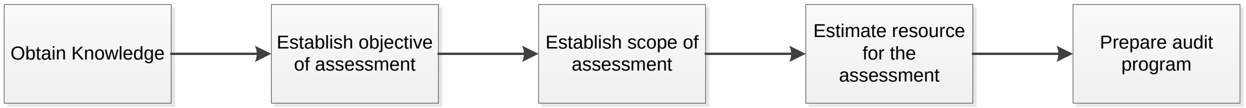
Planning step 1: Obtain knowledge of the NRREP technical component/ auditee

Planning step 2: Establish objective of the assessment

Planning step 3: Establish scope of the assessment

Planning step 4: Estimate resources for the assessment

Planning step 5: Prepare audit program


Obtain Knowledge
Establish objective of assessment
Establish scope of assessment
Estimate resource for the assessment
Prepare audit program

Details of each process have been explained below:

Planning step 1: Obtain knowledge of the component/ auditee

The internal audit team should obtain a sufficient level of knowledge of the NRREP Technical Component/ Auditee to identify important events, transactions, policies and practices that may have a significant effect on the financial information and activities of the Component / Offices. Following are some of the sources where from the internal audit team can obtain such knowledge:

- Previous experience with the auditee
- Legislation, circulars and regulations of donors/ GoN that significantly affect the auditee
- Auditee's policy and procedures manual and internal reports
- Visits to the Auditee's offices where the accounting and other documents are generated, maintained, and the administrative procedures followed
- Other documents followed by AEPC for example, subsidy delivery mechanism, circulars, manuals relating to accounting and internal controls, organizational charts, job description charts, etc.
- Performing process walkthroughs.

Planning step 2: Establish Objective of the assessment

The next stage in planning is establishing the specific objectives of the internal audit assignment. The establishment of such objectives should be based on the auditor's knowledge of the department's activity, especially:

- A preliminary understanding and
- Review of the risks and controls associated with the activities forming subject matter of the internal audit engagement.

Preliminary Understanding

The preliminary understanding involves gathering necessary information by means of a combination of the following procedures:

- Observation of the activity being performed
- Inquiry of the staff associated with performing the activity
- Discussion with the Institutional Head of the auditee

- Review of Organizational chart of the auditee
- Reading through the policies and procedures
- Reading through the Previous years' internal audit and OAG reports
- Performing analytical procedures (review of trends, ratios, budget vs. actual etc.)
- Performing actual walk-through tests

Review of the risks and controls

Internal audit team will have to perform risk assessment for auditee before undertaking the audit work. The objective of the risk assessment is to enable internal audit team to focus on areas of perceived risk within the organization. Internal audit team's role then is to apply the appropriate level of internal audit resources to the higher risk areas.

Internal audit team's role in risk assessment may vary depending on whether auditee has already performed a risk assessment.

- If a risk analysis has already been developed by auditee, Internal Audit team should assess that the risk analysis is appropriate, sufficiently recent, and that its scope is sufficient to address the main risks of the organization.
- If a risk analysis has not been carried out, the internal audit team should create one for the purpose of creating the audit programme.

The recommended risk assessment process for this purpose is designed to identify and analyze the inherent and specific control risks facing an organization. This approach is based upon an organizational risk framework called "ORCA," which is an acronym for Objectives, Risks, Controls and Alignment. During this exercise any internationally accepted Internal Control framework namely COSO may be followed.

Objectives - The auditee's overall objectives drive its activities and therefore relate directly to the most critical risks. As such, the first step in the ORCA framework is to understand the department's overall goals and objectives.

Risks & Controls - The next step is to identify the high level risks facing the auditee now and in the near term, categorizing each risk in terms of: likelihood of the risk occurring, and the impact if it did occur.

The internal audit team should also identify the underlying controls to mitigate the risks identified above through discussion and performing process walkthroughs. Based on the identified risks and controls, the internal audit team should prepare a Risk Control Matrix (RCM) for each of the processes within the department which should form the basis for any control assessment or internal audit activity.

Based on the assessment of likelihood and impact, an overall risk rating is assigned. This assessment is made prior to consideration of the strength of internal controls, risk monitoring activities, or processes surrounding the risk area. Overall risk assessment rating helps priorities the risks. Higher risk areas require more immediate attention by the internal audit team – either in the form of internal audit projects, or other risk monitoring activities.

Sometimes internal audit team may prefer to assess risk after the consideration of controls. In these instances, internal audit team should articulate the pros and cons of starting with residual risk to the Compliance unit. If the Compliance unit prefers to use residual risk after understanding the pros and cons, internal audit team should adjust their approach. Further explanation of inherent and residual risk is given below.

Alignment - The challenge in any organization is to mobilize individual and collective action toward achieving stated objectives. This requires alignment of an organization's strategies and objectives throughout its operational units, processes and people. The evaluation will focus on whether the controls appear to be effective in achieving the auditee's stated objectives and managing the related risks.

Risks can be categorized into three main categories:

- **Inherent or Gross Risk -** Inherent risk is the risk that exists in the process or audit area without considering internal controls. The assessment of inherent risk depends on the professional judgment of the auditor, and it is done after assessing the operating environment of the entity being audited. Items to consider when determining inherent risk include: complexity of the process or audit area, past audit results, the auditee's environment, and its overall risk awareness.

- **Residual Risk -** Residual risk is the level of risk remaining after considering relevant controls that have been applied to the inherent or gross risk.

- **Emerging Risk -** Emerging risks are large-impact, hard-to-predict and rare events beyond the realm of normal expectations. Example of emerging risks include:

    - Changes in laws and regulations (e.g. introduction of Goods and Services Tax etc.) that could cause an overhaul in the manner in which departments are run.

Internal Audit Team should identify emerging risks that are relevant to the auditee, assess their significance, interconnectedness with other risks and implications. Emerging risks should also be periodically monitored to understand potential changes in the likelihood or impact associated with the risk.

The internal audit team should use the information so gathered and result of risk assessment to determine the objective(s) of the engagement as also to decide the nature, timing and extent of audit procedures.

Planning step 3: Establish scope of the assessment

The scope of the audit should be sufficient in coverage so as to meet the objectives of the engagement. The internal audit team leader should consider the information gathered during the preliminary review stage to determine the scope of his audit procedures. In case the internal audit team is of the view that circumstances exist which would restrict them from carrying out the procedures, including any alternative procedures, considered necessary, Audit team leader should discuss the matter with the ISCA/ NCA to reach a conclusion whether or not to continue the engagement. The scope of engagement should be documented comprehensively to avoid misunderstanding on the areas covered for audit. The scope of audit should be discussed with ISCA/ NCA and the minutes of meeting must be included in the working papers.

In case of information technology based environment, the scope of engagement would include the extent to which internal audit team is permitted to access the system and reports which can be viewed and those which can be exported.

Further, system based audit tools that an internal audit team can use to draw and analyze data should be clearly stated in the scope of engagement.

Internal audit teams must ensure that the review is appropriately scoped to meet the objectives of the review and to confirm the review is delivered within budget.

When developing the scope of the audit, the internal audit teams should consider:

- Previous knowledge of the auditee and the results of previous audits
- Result of preliminary risk assessment
- Whether the review will cover the design and operating effectiveness of controls or testing only the design or operating effectiveness
- Fraud considerations

Planning step 4: Estimate resources for the assessment

Once the scope of the internal audit procedure is established, the next phase is that of deciding upon the resource allocation.

For this purpose, internal audit team should perform pilots to assess man-hour required to finish full-scope and limited scope audits. Based on the experience, the internal audit team should prepare an audit work schedule, detailing aspects such as:

- activities/ procedures to be performed;
- engagement team responsible for performing these activities/ procedures; and
- time allocated to each of these activities/ procedures.
- While preparing the work schedule, the internal audit team should have regard to aspects such as:
  1. any significant changes to the auditee's missions and objectives, operating processes, and its strategies to counter these changes, for example, changes in the auditee’s controls structure

  2. any changes or proposed changes to the governance structure of the auditee

- composition of the engagement team in terms of skills and experience

To measure actual time taken to perform a particular audit, internal audit team should implement a project (i.e. audit) wise time booking system for all the resources in the team.

Activity-wise work plan and resource allocation plan must be submitted to Compliance Unit during the planning phase for approval.

Planning step 5: Preparation of audit programme

The Audit team leader should prepare a programme listing the procedures essential for meeting the objective of the internal audit plan.

The internal audit programme should be designed so as to achieve the objectives of the engagement and also provide assurance that the internal audit is carried out appropriately.

The audit programme developed by the audit team leader would need to be a risk based audit programme, appropriately reflecting and addressing the priorities of the internal audit activity, consistent with the NRREP's goals. The audit programme shall be submitted to ISCA/ NCA at the beginning of audit.

Contents of audit programme

Previous audit results are an important input to the following year's audit programme. If audits have revealed a number of high-priority audit findings or if fraud has been identified, these areas should be considered for the new audit programme or for follow-up actions. High risk areas that have not been recently audited should also be considered for inclusion in the scope of the current audit programme.

In preparing the audit programme, the audit team leader and his team should ensure that the following aspects are covered:

- Governance – Audit team leader should assess and make appropriate recommendations for improving the accomplishment of the following objectives:
    - Promoting appropriate ethics and values within the auditee unit
    - Communicating risk and control information to appropriate sections of the auditee
    - Coordinating the activities of, and communicating information to the ISCA, Department Heads/ Heads of Offices
    - Evaluating the design, implementation and effectiveness of the auditee's ethics-related objectives, programs and activities
    - Assessing whether the information technology governance of the auditee sustains and supports the objectives
- **Risk management –** Evaluate and contribute to the improvement of risk management processes and also evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.
- **Control –**Assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement. This can

amongst other aspects include reviews of operations, determination of whether operations and programs are being implemented or performed as intended.

- **Results of previous audits –** If previous audits have revealed a number of high priority audit findings or if fraud has been identified, these areas should be considered for the current audit programme or for follow up actions.

The internal audit programme identifies, in appropriate details, the following:

- Objectives of the internal audit in respect of each area
- Procedures to be performed to achieve those objectives, i.e. a detailed work program or audit checklist
- Staff responsible for carrying out the particular activity
- Time allocated to each activity as also the sufficiently detailed instructions to the staff as to how to carry out those procedures.
- The internal audit programme may also have provision for information such as the procedures actually performed, reasons for not performing the originally identified procedures, actual time consumed in carrying out the relevant procedure, reasons for deviations from budgeted time etc.

The work program or audit checklist should be created or adapted from libraries of previously created audit checklist (if available) based on the scope. Audit checklist contains the main test steps to be followed during fieldwork that link the objectives, identified risks and controls and relevant recommended protocols. The audit checklist should be stored in the electronic work papers.

The work program or checklist should be updated throughout the fieldwork stage for any new information and identified issues.

3.3. Communication

A well-designed communication and reporting process is essential for the effectiveness of internal audit delivery. The communication plan is to be tailored for each audit and must form a key component of the service delivery plan.

The communication plan should include among other things, communication with internal audit stakeholders, including:

- International senior compliance advisor
- National compliance advisor
- Lead development partners
- NRREP Steering committee

A Communication Plan essentially shall focus on following aspects:

- How to communicate with various stakeholders
- What to communicate
- When to communicate
- Communication with team members

How to communicate

A communications plan provides a coherent and consistent approach for how, what and when audit teams communicate with the Compliance Unit, auditee and donors.

It helps by:

- Enabling Compliance unit and auditee to be an integral part in co-developing mutual expectations
- Establishing protocols up front by agreeing how, what, and when the audit team will communicate throughout the audit.
- Establishing a uniform format for planned communications.

What to communicate

Audit teams should use the communication plan to:

- Set the tone for the relationship
- Lay the foundation for communication with the ISCA, Head of relevant Technical Component and auditee.

Communication to various stakeholders is to be done as outlined above.

To maintain the surprise element in the audit process (to avoid ‘managing’ the records), the audit team should communicate the audit plan and timing three days prior to commencement of audit. Details of scope and approach should only be discussed during the Opening Meeting with the auditee.

When to communicate

Internal audit needs to stay up-to-date on developments affecting the overall risk profile of various components under NRREP and discuss emerging risks with technical component manager. Technical component managers should have regular contact with internal audit teams.

A contact "owner" should be identified on the internal audit team who will be responsible for maintaining contact with the identified member of component and for determining the desired frequency of contact.

The frequency and formality of meetings should be set up keeping in view the risk in the area under consideration, size, complexity of responsibility for the area, the level of change being experienced in the area.

Internal communication among the audit team members

Communication should happen from the Audit manager for giving the team directions, monitoring the team’s progress discussing any issue of significance. Team meetings are of three types as explained below:

Kick-off Meeting

All key team members should organize a kick off meeting to discuss the audit objectives and the key tasks to be undertaken during the conduct of Internal Audit.

This meeting will allow the team to identify and understand the events, transactions and practices that, based on their judgment and experience, may have a significant effect on the activities of the auditee.

The objective of this meeting, amongst other things is, for the audit team to get the understanding of:

- the potential for fraud or error in the specific areas assigned to them, and
- how the results of the audit procedures that they perform may affect other aspects of the audit including the decisions about the nature, timing and extent of further audit procedures.

The more experienced audit team members will share their insights based on their knowledge of the entity, and for the team members to exchange information about the risks to which the entity is subject.

Taking Stock Meeting

At the “taking stock” meeting there should be a discussion of what evidence has been obtained and an update on the understanding of the auditee’s process and procedures.

The senior team members must be present in these meetings besides the team members who are involved in audit fieldwork.

The senior team members should consider whether audit tests have been done properly, whether any further work needs to be done based on discussions with auditee and whether the outcome of those tests needs to be communicated to the auditee at once, or later during the audit process. The number of meetings held in any audit and who should attend will vary with the circumstances of the entity and audit team. These meetings are vital to maintain and monitor quality of execution and minutes of meeting must be recorded to demonstrate that regular reviews were conducted during the audit by the senior audit team members.

Debrief Meeting

After the fieldwork is substantially complete, a team meeting should be held. Audit manager should debrief the entire audit team on the results of the work and any issues addressed.

The audit manager should ensure that an internal debriefing meeting is timely planned and conducted, encouraging the participation of all team members. Full participation of the team contributes to a comprehensive assessment of performance.

The audit team should maintain minutes of these team meetings and the meetings with the auditee in the engagement file to update the risk assessment, brief the compliance unit and NRREP steering committee, and prepare for additional meetings.

3.4. Assessment and execution

Once the scoping and planning is completed the audit team will begin execution. This phase includes a review of control design, controls testing, and assessing the root cause of any issues identified.

Methodology for Execution

Methodology for audit execution will include the following steps:

- Gain an understanding of the flow of transactions through the process or system[1]
- Evaluate whether the controls are designed adequately
- Identify and test key controls to assess whether or not they are operating as designed
- Discuss preliminary findings and conclusions with the auditee throughout fieldwork

Opening meeting

An opening meeting is important to discuss the audit objectives, scope and timing with the auditee and to obtain their buy in to the process. It is important to communicate the areas to be audited, relevant time period for the audit to the auditee during the opening meeting.

Attendees at this opening meeting normally include:

- Auditee managers
- Key personnel associated with the process under review
- Concerned head of auditee organization

The discussions of the opening meeting should be captured in minutes and retained in the work paper file.

Control design

Understand the process

The audit team needs to understand the flow of transactions through a system or process especially related to subsidy disbursement. This may, but does not always, include how transactions are initiated, recorded, authorized, processed and reported. The team should gain an understanding of:

[1] Refer chapter 4 of this manual for illustrative documents to be referred to understand flows of information in the transaction system.

- How system or process objectives are defined, communicated, measured and monitored
- Key phases or stages of the system or process
- Key risks that may prevent the achievement of the system or process objectives, including fraud risk
- Key documents produced during the subsidy disbursement process
- Movement of subsidy disbursement documents from one stakeholder to another
- Retention and documentation of subsidy disbursement documents

System or process document comprises of, but is not limited to:

- Financial management guidelines of NRREP
- Subsidy disbursement mechanism
- Financial management guidelines of Auditee

Auditee already has systems or process documentation. The audit team by performing a walkthrough with the process/system owner should assess whether the manual /process documentation is accurate. Verification of the system or process documentation will enable the audit team to make judgments as to which controls should be evaluated.

Evaluate control design

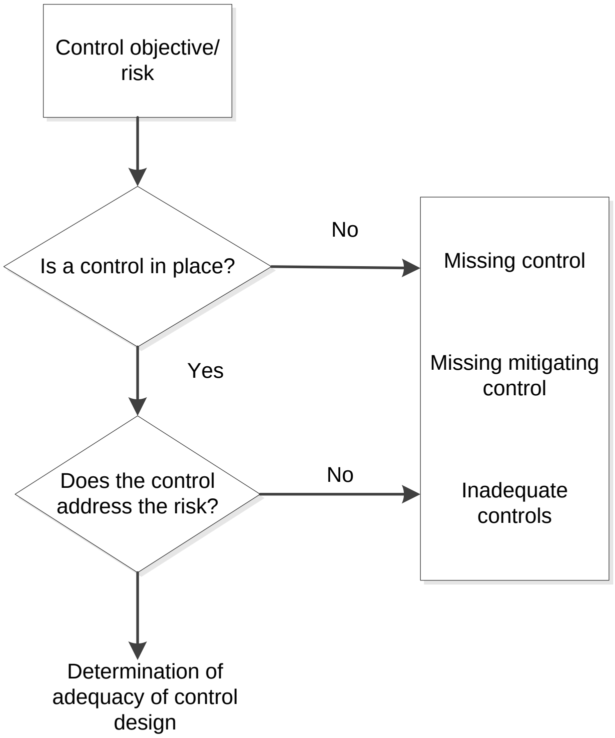
The Audit Team should evaluate the existence of controls and adequacy of design effectiveness.

To map controls to their related risks and objectives, the internal audit team use the Risk and Control matrix format. Refer annexure – II for an illustrative design of risk and control matrix format.

Using the matrix, internal audit teams are able to identify missing controls that should be in existence to mitigate a key risk and/or duplicative controls that could lead to process inefficiencies.

When evaluating design effectiveness of internal controls, the following factors have to be considered:

- **Alignment between the controls and the risks identified –** The evaluation will focus on whether the controls appear to be effective in achieving the stated objectives of the NRREP/ technical component and managing the related risks.
- **Nature of the control –** Whether the control procedure is detailed enough to control the risk. For example, a high-level departmental performance review rarely provides sufficient evidence to be considered an effective control, but properly designed detailed processing controls should provide sufficient evidence.
- **Follow-up actions taken by the auditee –** For a control to be effective there needs to be adequate follow-up of issues and exceptions, in a timely manner.
- **Frequency of the control –** This will affect whether the control will detect or prevent the risk identified on a timely basis.
- **Period covered by the control –** For audit purposes, it may be necessary to obtain evidence that a control is effective for the specified period in which the risks are relevant.


Control objective/ risk
Is a control in place?
No
Missing control
Yes
Missing mitigating control
Does the control address the risk?
No
Inadequate controls
Determination of adequacy of control design

Control testing

Once a control is determined to have been adequately designed, it is subject to testing in order to determine that it is operating as designed.

Risks may be mitigated through multiple controls; however, not all of those controls necessarily need to be tested. The audit team should focus on the controls with the highest potential impact on risk mitigation.

Control testing objectives

Tests of controls are designed to obtain evidence to assess their operating effectiveness. Operating effectiveness means that the controls procedures within the auditee are functioning on a consistent basis as designed.

The test objective should identify the control and state the attributes to be evaluated, as follows:

- Was the control executed correctly to mitigate the associated risk(s) and meet the related objectives of the auditee/ NRREP?
- Did the correct person perform the control?
- Was the control performed consistently during the period under examination?

Time period over which the testing is to be performed

When determining the period over which control testing will be performed, the following should be considered:

- Periods when controls may not be operating effectively, such as during holiday periods of key personnel or periods of high turnover, significant changes in auditee's organization structure or system conversions
- Change in controls during the period under audit
- New systems

Testing techniques

There are four basic testing techniques to test the controls. The four testing techniques are as follows:

- inquiry,
- observation,
- examination of evidence, and
- re-performance

The audit teams should choose one or more types to obtain audit evidence.

These audit procedures may be used to identify and assess risks, or serve as an evaluation of controls, depending on the context in which they are applied. The testing technique selected depends on the degree of assurance required by the auditor.

Inquiry

Inquiry consists of seeking information of knowledgeable persons within the auditee organization. Evaluating responses to inquiries is an integral part of the inquiry process. Inquiry involves:

- Considering the knowledge, objectivity, experience, responsibility and qualifications of the individual to be interviewed
- Asking clear and concise questions to understand how a control has been applied (e.g. when, how often, with what data)
- Identifying whether the individual understands the appropriate objectives of a control procedure (e.g., by asking about typical or expected errors, follow-up protocols and transactions that do not follow the normal procedure)
- Using open-ended or closed questions appropriately
- Considering the interviewee's responses and asking follow-up questions

Inquiry is usually required when seeking to understand whether a manual control that involves judgment has been properly applied. For example, inquiry of a member of the auditee who approves reconciliations or transactions can help determine whether the individual understands what should be identified for follow-up and whether the approval process has been done diligently. Interviews or questionnaires can be used for inquiries.

Inquiry alone ordinarily will not provide sufficient audit evidence to detect the presence of a control or to support a conclusion about its operating effectiveness. Internal audit should consider performing tests in addition to the use of inquiry to obtain sufficient appropriate audit evidence.

Observation

Observation consists of looking at a process or procedure being performed by others. Examples include observation of the physical counting of stores items by the auditee's personnel or observation of the performance of control procedures that leave no audit trail. Observation provides audit evidence about the performance of a process or procedure, but is limited to the point in time at which the observation takes place and by the fact that the act of being observed may affect how the process or procedure is performed.

Examination

Inspection of information or data – Inspection consists of examining records or documents whether in paper form, electronic form, or other media. Inspection of records and documents provides audit evidence of varying degrees of reliability, depending on their nature and source and, in the case of internal records and documents, on the effectiveness of the controls over their production.

Walkthroughs – A walkthrough is a method of confirming understanding of a process flow by tracing an individual transaction from beginning to end. For example, following a subsidy disbursement transaction from origination through the auditee's information system until it is reflected in the financial reports of the relevant technical component. A walkthrough can be used to confirm understanding of the design of controls. Much of the walkthrough will be examination of documents but may also include:

- Making inquiries of the person that performs the procedure or control
- Observing the performance of the procedure or control
- Reviewing documents that are used in, and that result from, the application of the procedure or control
- Comparing supporting documents (i.e. subsidy disbursement forms, contracts and calculation of subsidy form) to the accounting records.

Re-performance

Recalculation – Recalculation consists of checking the arithmetical accuracy of documents or records. Recalculation can be performed through the use of CAATs (Computer Assisted Audit Techniques), for example, by obtaining an electronic file to check the accuracy of the summarization of the file. Recalculation of subsidy calculation is a key test that can be performed while testing subsidy disbursement controls.

Re-performance – Re-performance is the independent execution of procedures or controls that were originally performed as part of the auditee's internal control. Re-performance techniques are often the most time consuming to undertake.

Determine which testing technique should be used

When an internal audit team is testing internal controls, it is seeking sufficient assurance to suggest valid findings and recommendations on the design and/or operation of controls, based on the scope set out in advance and agreed upon with the auditee and compliance unit.

A combination of techniques may be used. Which techniques to use depend on many factors, but primarily should be based on:

- **The nature of the control, in particular the degree of susceptibility to change.** A control that is susceptible to change usually should not be observed as the observation may not be representative of the control's operation under normal circumstances. For example, control over procurement process which needs to be checked by way of examining the documents for individual cases and not by way of observation.

- **The frequency and extent of the control.** A control that operates infrequently and requires a significant effort, such as a physical count of stores items, should not be re-performed because of the impracticability of doing so but may be observed.

- **Initial view of the likelihood of control weakness, based the assessment of the control's design.** For example, it may be concluded that a control is highly unpredictable based on its manual nature, past failures, or complexity of process. In this case, re-performance may be preferred to capture the variations in the process.

- **Significance of the control to the control environment and how much reliance is being placed on it.** For example, efficacy of control over tendering process should not be checked by way of inquiry or observation but by way of examining the documents.

Sampling

"Audit sampling" means the application of audit procedures to less than 100% of the items in a population of transactions to enable the internal audit team to obtain and evaluate audit evidence about some characteristic of the items selected in order to form a conclusion concerning the population.

Sampling approaches can either be statistical or non-statistical in nature.

The sampling guidance detailed below, is directed to non-statistical sampling applications but grounded in statistical theory. It is designed to provide:

- The necessary information to determine appropriate sample sizes and selection techniques,
- Evaluation of results from non-statistical sampling.

Sampling risk

"Sampling risk", means the risk that the internal audit team's conclusions, based on examination of a sample may be different from the conclusion reached if the entire population was subjected to the same types of internal audit procedure.

The two types of sampling risk are -

(a) The risk that the internal audit team concludes that controls are more effective than they actually are.

(b) The risk that the internal audit team concludes that controls are less effective than they actually are, or that a material error or misstatement exists when in fact it does not.

Sampling risk can be reduced by increasing sample size.

Sampling period

As a general guideline, the analysis should be performed on activity over the appropriate period. For financial reporting findings this usually means since the start of the current fiscal year. For operational findings the period may vary depending on the duration of the process.

The test objective may also influence the timing of the analysis. For example, analysis that is designed to assess a specific transaction should be focused on the specific timeframe of that transaction.

Non-statistical sampling

There are three key steps in a non-statistical sampling process:

- Determine the control test objective, population and sampling unit
- Determine the sample size
- Select the sample for testing

Determine the sample size for manual controls

The following guidance related to the frequency of the performance of control may be considered when planning the extent of tests of operating effectiveness of manual controls for which control deviations are not expected to be found. The internal audit team may determine the appropriate number of control occurrences to test based on the following minimum sample size for the frequency of the control activity dependant on whether assessment has been made on a lower or higher risk of failure of the control.

Frequency of control activity	Minimum sample size	
	Risk of failure	
	Lower	Higher
Annual	1	1
Quarterly (including period end i.e. +1)	1+1	1+1
Monthly	2	3
Weekly	5	8
Daily	15	25
Recurring manual control (multiple times per day)	25	40

*Sampling size prescribed is per the SIA 5 promulgated by Institute of Chartered Accountants of India

Sampling methodology for testing control activity

The following factors may be indicative that a larger sample size should be considered:

- The greater the potential financial loss or adverse event to the auditee/ NRREP if the control is not effective or fails
- The more complex the control
- The greater significance of judgment in control operation.

Sample sizes for automated controls

The testing of manual controls is generally more extensive than the testing of automated controls. In some instances, provided that general computer controls [2] have been tested and are deemed to be effective, the testing of a single operation of an automated control is sufficient to determine its effective operation. If the engagement team has already completed a review of the system's general computer controls, which has indicated that they are effective, then the engagement team would only test the system once to assess that it, indeed, performs this check.

However, the extent of manual investigation of the exceptions would be determined by reference to the above sample size ranges for testing manual controls.

Select a sample

The objective for any sample selection method is to obtain a representative sample of the population. To increase the likelihood that a sample will be representative, all items in the population should have an equal opportunity of being selected. Common methods of selecting a sample, using a non-statistical sampling approach, are as follows:

Random selection

- This is a method where all items in a population have an equal chance of being selected.
- Random selection involves no human judgment, and is therefore a preferable selection technique as it excludes bias.
- Random number software, including Microsoft Excel, can be used to select the sample.

Haphazard selection

Haphazard selection is a method for selecting a representative sample size using judgment. The auditor, without any conscious bias, selects sample items randomly, (i.e. without any special reason for including or omitting items from the sample). This may be an acceptable

[2] General Computer Controls are those that are not specific to any particular IT application. These deal with controls around Computer Program development, Program Change, Access related Controls, Computer Operation related Controls.

alternative to random selection when electronic data is not readily available and if there is confidence that selection conditions will not induce bias.

On completion of the process and controls testing, the team member should evaluate exceptions or errors identified in terms of the following:

- The potential effect on control objectives of identified errors or exceptions
- The incidence, or level of error found
- The cause – what was the root cause of the control breakdown?
- Actual effect – if applicable and it can be determined.

Identify root cause

The key to delivering high quality audits extends beyond identifying areas of control breakdown to providing high quality, practical recommendations that address the root cause of the issue identified.

A root cause analysis should be performed to understand the reason behind the breakdown in controls (e.g. if issues occurred in a specific period of time there may be a discrete identifiable cause). Next, an assessment should be made as to whether the conditions which led to the breakdown in controls still exist.

The recommendation raised to address the issue should be determined based upon the reason for the breakdown in controls. For example, if stores and assets have not been physically verified for years in a unit, one needs to understand the specific reason behind it. That is, whether it was shortage of manpower or lack of awareness of the process or some other reason.

Common causes of breakdowns of internal control relate to:

- People – competency, human error, demand on time or deliberate fraudulent acts
- Systems – security, suitability, stability or functionality
- Internal environment – Auditee's culture, working conditions or performance pressures
- External factors – unexpected events, regulatory environment or economic factors

Finalize

The following activities need to be performed to finalize audit fieldwork:

- Discuss the accuracy of findings with the auditee prior to completion of field-work.
- Hold a formal closing meeting with auditee.

Validate findings during the closing meeting

Once the execution phase has been completed, the findings need to be finalized. Although issues should be discussed throughout the audit with the auditee, presentation of the issues in writing for finalization generally occurs during the closing meeting.

A closing meeting serves the following purposes:

- Confirms that the issues raised are factually correct
- Allows the auditee to discuss and comment on findings
- Prevents surprises when the draft report is issued
- Allows the team to discuss options for practical recommendations

Audit action plans

The audit team should evaluate which issues and findings identified during the audit should be reported, even if auditee has already addressed the issue before the audit report is issued. If the auditee has already addressed the issue the report should contain details of the auditee's actions already taken.

Audit action plan should address the root cause identified by the audit team.

If the audit team determines that a finding does not need to be reported, the rationale must be documented in the work papers. In all cases, unreported findings should remain in the audit documentation, unless clearly inconsequential.

Where issues have not already been addressed, auditee should develop an action plan which should include:

- A statement of what actions will be taken
- The timeframe of actions to be taken
- Who will perform the various actions

3.5. Reporting

The internal audit report is the most visible record of internal audit's performance. It is therefore vital that this internal audit report is of high quality.

This section outlines requirements for format and content of internal audit reports, as well as the process by which reports are written, edited, and finalized.

This section also outlines wrap-up procedures, considerations for communicating results to the following:

- Compliance Unit
- Technical component managers
- Auditee

Detailed reporting

The following steps are to be performed by the audit team for the purpose of reporting:

- Develop the draft internal audit report and obtain approval from National Compliance Advisor before issuance to the auditee.

- Obtain International senior compliance advisor's and Component manager's comments.
- Finalize the internal audit report and obtain International Senior Compliance Advisor's approval before issuing to the auditee.
- Confirm audit findings documented in the report have appropriate component's action plans.

Reporting guidelines

Following the closing meeting, the audit team should prepare a draft report to issue to Technical Component Head for formal comment and agreement of remedial actions to be taken.

The following practices should be followed in drafting a well-written report:

- **Accuracy –** reports should be supported with facts. It is extremely important that the credibility of each audit be maintained by factual, unbiased and objective reporting.

- **Clarity –** reports should be understandable and clear. Reports should not require interpretation or oral comment to fill in the gaps. The report should stand by itself.

- **Quantification –** comments should be quantified to the maximum extent possible to provide the Compliance unit with a view of the significance of the findings. Examples of quantification are value amounts, number of test exceptions and scope of testing.

- **Conciseness –** reports should be to the point, but this does not necessarily mean short.

- **Fairness** – reports should maintain a diplomatic balance with respect to the sensitivities of all readers. Observations should be fact-based and result in improvement recommendations, not in criticism of people, processes or systems.

- **Timeliness –** reports should be issued in a timely manner upon completion of the assignment.

- **Resolution –** the Technical Component manager's comments should indicate who in the Component is responsible for remedial action, and when it will be complete. Without specific responses and assignment of responsibility, the effectiveness of the audit and findings will be lost.

Individual finding ratings

Internal audit team may provide a rating against each of the issues raised in the report. Determining the severity of an audit finding is a combination of the probability of occurrence and the significance of the impact. Individual observations that by themselves are not severe and that have a common root cause should be grouped together and given a higher rating indicating the combined risk.

It is the responsibility of the concerned audit team leader to assess whether audit findings will be reported. If the finding need not be reported, the rationale should be documented in the work papers. In all cases, unreported findings should remain in the audit documentation, unless clearly inconsequential.

Report content

Audit reports submitted to Compliance Unit by internal audit team shall normally include:

Addressee: The report should be addressed to International Senior Compliance Advisor

Background and scope: This section of the report should provide a summary of why the audit was conducted or selected (e.g. part of normal audit plan, special project at the direction of Compliance Unit/ Donors or AEPC, fraud investigation, etc), the element, process, component or operational unit subject to the audit, the general timeframe of the audit, special factors encountered during the audit and impact on the process, and any other considerations the reader should be aware of when reviewing the findings included in the report.

Limitations and responsibilities: This section of the report sets out the limitations on the level of assurance internal audit can provide and an explanation of the responsibilities of internal audit and Compliance Unit.

Findings and recommendations: This section is normally a table with column headings of, observations, root cause, risks, recommendations and action plans.

- **Observations –** Specific details about when and where the problem was occurring. It should be supported with factual data of what was observed or result of tests completed
- **Root Cause –** The underlying root cause or the reason behind the breakdown in controls
- **Risks –** Specific risks that the auditee is exposed to as a result of breakdown in controls
- **Recommendations –** Recommendations should be relevant and practical and should address the root cause of the finding. Before recommendations are proposed, the benefits should be compared to the cost of implementation. The issues which need to be dealt at policy level should be highlighted.

While it is the responsibility of the Auditee to decide whether the implementation of a recommendation is justified, the internal audit team should not exclude any significant control weaknesses from the report simply because resolution would be costly. More than one recommendation may be required to completely address an issue.

Recommendations should:

- Remediate the control deficiency by addressing the root cause rather than the symptoms noted
- Improve alignment between risks and controls

Reporting timeline

Report distribution – Internal control weaknesses identified should be communicated to appropriate personnel in the auditee unit and a copy should be marked to relevant Technical

Component Manager. A written report should be delivered to the Compliance Unit head (International Senior Compliance Advisor). The internal audit team should also consider communicating key findings to the Head of AEPC.

For easy access and virtual storage, digital copy audit reports may be kept in the custody of National Compliance Advisor and International Senior Compliance Advisor. Access to the storage location may be restricted through password to maintain confidentiality.

Dating of reports – The date of internal audit report should be the date of fieldwork completion. The end of fieldwork occurs at the completion of the testing and execution phases of the audit, including when a completed draft of the report with findings and recommendations is discussed with the auditee in a formal closing meeting.

If information is provided in the closing meeting or subsequent to the closing meeting that requires internal audit team to perform further review and testing or increase scope, then the end date for fieldwork occurs when the additional testing and discussion is completed. The report date should not be extended for activities such as compiling the report or incorporating auditee comments or responses to the findings or recommendations.

Review by concerned technical component manager – Concerned Technical component manger in NRREP should review the report in its entirety and discuss significant findings with members of the audit team, as necessary. This review should be evidenced on the report and/or work papers.

3.6. Documentation

The internal audit team should document matters, which are important in providing evidence that the audit was carried out in accordance with the methodology and support the findings or the report submitted by them. In addition, the working papers also help in planning and performing the internal audit, review and supervise the work and most importantly, provide evidence of the work performed to support the findings or report(s).

What should be documented?

Internal Audit documentation should clearly denote:

a) terms and conditions of an internal audit engagement, scope of work, reporting requirements, any other special conditions, affecting the internal audit;

b) the nature, timing and extent of the audit procedures performed to comply with methodology and applicable legal and regulatory requirements;

c) the results of the audit procedures and the audit evidence obtained; and

d) Significant matters arising during the audit and the conclusions reached thereon.

The documentation prepared by the internal audit team should be such that enables an experienced person (or a reviewer), having no previous connection with the audit to understand

and reach at the same conclusion by performing the steps documented in the file (this is called **re-performance standard**).

It is, however, neither necessary nor practicable to document every matter the audit team considers during the audit. Audit documentation should be enough to support the fact that work has been done to satisfy the Audit Objectives and evidence gathered to support that conclusion on the effectiveness of processes/controls.

Items to be documented

The internal audit documentation should cover the entire engagement viz., engagement planning, risk assessment and assessment of internal controls, evidence obtained and examination/ evaluation carried out, review of the findings, communication and reporting and follow up. Ideally documents relating to the auditee, which may be required in the future years, should be kept separately in a permanent file and documents specific to the current year audit should be kept in a current working file.

Permanent files shall include the following:

- Copies of significant contracts and agreements or auditee representations on terms and conditions of those contracts.
- Copies of relevant circulars, extracts of legal provisions
- Evaluation questionnaires, checklists, flowcharts, etc
- Papers relating to discussions/ interviews with the various personnel including legal experts, etc
- Chart of the auditee's organizational structure, job profile of the persons listed in the chart and rules of delegation of powers
- Results of risk and internal control assessments

Current file shall include the following:

- Internal audit plan and programme for the current year
- Papers relating to the staff requirement and allocation including requirement of technical experts, if any
- Time and cost budgets
- Internal review reports
- Annual budget and development plan
- Progress report, MIS report
- Reconciliation statements
- Communication with the auditee and third parties, if any
- Certification and representations obtained from the auditee
- Audit procedures performed and results thereof
- List of queries and resolution thereof
- Copy of draft audit report, along with the comments of the auditee thereon and final report issued
- Records as to the follow up on the recommendations/ findings contained in the report

Finalization of documentation

The internal audit documentation should identify the following:

i. who performed that task and the date such work was completed;
ii. who reviewed the task performed and the date and extent of such review;
iii. reasons for creating the particular internal audit documentation;
iv. source of the information contained in the internal audit documentation; and
v. any cross referencing to any other internal audit documentation.

The preparers and reviewers of the internal audit documentation should also sign them. The internal audit file should be completed within 30 days after the signing of the internal audit report.

Completion of the internal audit documentation file is only an administrative process and does not involve performance of any new audit procedures or formulation of new conclusions. Changes may be made to the audit documentation file only if such changes are administrative in nature. For example:

- deleting or discarding superseded documentation;
- sorting, collating and cross referencing internal audit documentation;
- signing off on completion checklists relating to file assembly process; and
- documenting audit evidence that the internal audit team has obtained discussed and agreed with the relevant members of the audit team before the date of the internal audit report.

When exceptional circumstances arise after the date of the submission of the internal audit report that require the internal audit team to perform new or additional audit procedures or that lead the internal audit team to reach new conclusions, the internal audit team should document:

- the details of circumstances encountered along with the documentary evidence, if any, thereof;
- the new or additional audit procedures performed, audit evidence obtained, and conclusions reached; and
- when and by whom the resulting changes to the audit documentation were made, and (where applicable) reviewed.

Document retention and access

The Compliance Unit should formulate policies as to the custody and retention of the internal audit documentation within the framework of the overall policy of NRREP in relation to the retention of documents. The Compliance Unit retains the ownership of the internal audit documentation.

While formulating the documentation retention policy any legal or regulatory requirements in this regard also need to be taken into consideration. Designated personnel from the respective component of NRREP may seek access to the internal audit documentation of the Compliance Unit subject to the approval of the International Senior Compliance Advisor.

After the assembly of the audit file, the internal audit team should not delete or discard internal audit documentation before the end of the retention period.

3.7. Follow up

Follow-up audits are designed to determine whether corrective action has been taken on previous audit recommendations. These audits may be conducted at the direction of the Steering Committee six months after a Final Audit Report was issued and usually include only the deficiencies reported in the Final Audit Report. The follow-up audit may include such functional or substantive tests that are necessary to verify that logical and appropriate corrective actions have been taken.

Audit issue tracking

The following activities need to be undertaken for Audit Issue Tracking:

- Perform audit issue follow up with the auditee on a regular basis
- Develop a protocol with appropriate level of the auditee to report overdue audit actions to the International Senior Compliance Advisor

Follow-up procedures provide the Compliance Unit with updated information about whether key risks have been properly mitigated through remedial actions.

Follow-up tracking system should be established and include at a minimum:

- Individual records for each recommendation
- Name and contact information for the process/ person who agreed to implement the required remedial action
- Original and any revised target dates for implementation

4. Compliance Reviews

Auditing is an inherent element of good governance, transparency; prudent management of both private & public funds and contributes towards affirming accountability thereof. It is imperative for the Compliance Unit to instil a faith and trust amongst the management, owners, taxpayers, financiers, legislature, executive, ordinary citizens and other stakeholders for the funds being expended, accounted and audited as per the guidelines and mandates governing the expenditure. In addition, Compliance Unit has to continually ensure transparency in operations and 'value for money' is achieved.

Internal audits to be conducted by the Compliance Unit: A risk based internal audit shall mainly focus on reviewing the robustness of current level of internal controls, checks and balances embedded in various financial and operational process. It also includes review of compliance with applicable policies, plans, procedures, laws, and regulations that could have an impact on operations.

Internal Audit is well placed as an important and integral element of a robust financial management with responsibilities to review, appraise and provide management with reasonable assurance on the adequacy of internal controls and risk management within an entity. A world class internal audit function is built on the following key pillars:

- **Knowledge systems**: Knowledge is fundamental to quality service in execution of performance, operational, financial, forensic, and other value-chain internal audits. Knowledge database and transfer includes the following key components:
  - Sector/industry risk analysis and indicators
  - Normative business process models
  - Leading practice monitor and risk strategies
  - Sector/industry knowledge networks
  - Centre for business knowledge & repository
- **Technology enhanced efficiency**: Leveraging the technology enablers through:
  - Enhancing efficiency through by delivering more thorough analyses and accurate conclusions
  - Focussed identification of significant business risks and audit scoping
  - Effective communication enablers
  - Business insights and process improvement suggestions
  - Process enhancements through data analytics, service delivery, assessments and security
- **Risk based methodology**: Focus on long term process refinements and business process engineering rather short term transaction based issues and fault finding mechanism
- **Quality assurance**: A good internal audit function is based on established quality assurance and improvement programme through quality assessments, ongoing internal monitoring and assurance to compliance to the standards

- **Reporting framework**: Existence of an independent, objective, ethical reporting, communication and follow-up framework

Thus, an internal audit function would include:

- Independent positioning of audit function
- Risk focus audit of processes aligned to needs
- Source of advice on governance, risk and controls
- Adequate coverage of functions, transactions and processes
- Qualified adequate resources
- Leverages IT tools

The aforesaid objectives can be achieved by the Compliance Unit through the conduct of variety of audits. Various types of audits typically conducted by the Compliance Unit shall be:

- Financial reviews: It includes reviews of the reliability and integrity of financial and operating information through financial statements audit. It provide reasonable assurance that the financial statements of an entity present fairly the financial position, results of operations, and cash flows in conformity with generally accepted accounting principles
- Procurement reviews: A procurement review is a holistic review of the existing capacities, internal controls and readiness of the auditee in its procurement process. Procurement reviews include assessment of the current state of implementation and effectiveness of pre-defined policies, guidelines. Performance Audit: Performance auditing is concerned with the audit of economy, efficiency and effectiveness of administrative principles, practices and management policies
- Performance reviews: As per the International Congress of the Supreme Audit Institutions (INTOSAI) auditing standards, Performance auditing embraces (i) Audit of the economy of administrative activities in accordance with sound administrative principles and practices and management policies; (ii) Audit of the efficiency of utilization of human, financial and other resources, including examination of information systems, performance measures and monitoring arrangements, procedures followed by audited entities for remedying identified deficiencies; and (iii) Audit of the effectiveness of performance in relation to achievement of the objectiveness of the audited entity, and audit of actual impact of activities compared with the intended impact. The basis of performance auditing is accountability to the stakeholders who have invested (financial or otherwise). Public accountability means that those in charge of a government program or ministry or fund or an entity's operations and / or funds are held responsible for the efficient and effective running of such responsibility.
- Regulatory reviews: A regulatory review shall include a systematic and objective examination to determine compliance with technical subject matter such as environmental audit, energy audit, technology audit etc. This may also include special audit such as forensic audit etc.

On the basis of the reviews as conducted in accordance with this Chapter, the Compliance Unit shall identify the risks, mitigation plans, residual risks etc for the purpose of MIS reporting under Chapter 5. Compliance Unit shall also refer the Internal Control-Integrated Framework of Committee of Sponsoring Organisations of the Treadway Commission to prepare a framework which enable the auditees to effectively and efficiently develop maintain a system of internal control that can enhance the likelihood of achieving the objectives of a transparent and good governance in the administration of its own and NRREP goals and adapt to changes in the business and operating environments.

4.1. Financial Review

Scope

The scope of financial review shall encompass the examination and evaluation of the adequacy and effectiveness of the auditee organisation's system of internal control and the quality of performance in carrying out assigned responsibilities.

The financial review team shall examine books and accounts to verify the accuracy and completeness of accounts to ensure that:

1. All revenues and receipts are fully and properly collected and are brought to accounts under the proper heads;

2. All expenditure and disbursements are authorized, vouched for and correctly classified, and

3. The accounts represent all financial transactions completed during the year accurately.

The financial review team shall also:

1. Review the processes and control systems established in the various departments of auditee to assess the degree of compliance with those policies, plans, procedures, laws, and regulations which could have a significant impact on operations and reports;

2. Determine whether the existing system of controls around spending are appropriate considering the structure of the auditee;

3. Review the means of safeguarding assets and, as appropriate, verify the existence of such assets. The objective of the auditee's departments is to ensure that assets are reasonably and adequately protected against loss and that they are properly managed and accounted for. The safeguard of assets shall not be restricted to mere pilferage but also include safeguards against physical threats like fire, water, electricity, etc.

4. Review operations or programmes undertaken by the various auditee departments to ascertain whether results are consistent with established objectives and goals and whether the operations or programs are being carried out as planned;

5. Ensure adherence to action plans as recommended and agreed during previous internal audits/ financial reviews through follow-up, reviews etc.

Coverage

The financial compliance review shall cover all the financial transactions for immediately preceding financial year and for the financial year in which financial compliance review is conducted. Coverage of all financial transactions primarily means that none of the financial transactions are outside the scope of financial review and for the purpose of conducting audit sample size for testing must be decided as per the sampling guidance in chapter 3. The review shall also cover the financial transaction recording system used to capture financial transactions. Financial compliance review shall cover all aspects of the financial management system starting from budget planning/ preparation, accounts management, cash/ fund management, hire to retire, fixed asset management and subsidy management etc. Guidance for select components of financial management system review is provided in the following section.

Budgeting review

Budget review shall focus on the robustness of budget planning process in the auditee department/ entity. It is important to review this area of financial management as budget is a tool for planning yearly activities and also serves as a control tool for expenditure during the year. During the review of budgeting process the auditor shall focus on the following:

- Controls in the budget process
- Budget preparation guidelines
- Monitoring and review of the budget preparation process
- Forecast tools and trend analysis to estimate the expenditure and revenue
- Inclusiveness of the budget planning process
- Level of detail in budget planning process

Illustrative risks and control tests for budget process are as follows:

Risk	Tests to be performed
Budget model/system not up-to-date and in line with structural and operational changes	- Review the budgeting template against corporate guidelines and also against the available accounting heads for correctness and comprehensiveness
Irrelevant/inaccurate assumptions and factors underlying the budgeting model/system	- Review the consistency in application of various assumptions/factors by comparing budgets for different periods. Comment on relevance of these assumptions/factors
Relevant people not involved in the process of determining accurate and realistic budgets	- Review the budget determination process and ascertain how the inputs of various departmental heads were included in the budget
Classifications/groupings not comparable while performing budget to actual review	- Establish if the standard classification/clubbing is used while preparing budget file and computing actual figures to ensure effective comparison. Assess the process to prevent unauthorized or invalid adjustments to the budget or actual figures
Budget versus actual comparison not	- Review the effectiveness of timely

Risk	Tests to be performed
circulated/reviewed on a timely and prompt basis	communication of the budget versus actual comparison - Review the circulation list for this comparison to ensure that this sensitive information is protected from unauthorized exposure - Establish instances where budget was exhausted for a particular expense item and then incremental expense for this line item was booked in another code

Accounting framework review

Accounts management is a key activity and becomes the basis for preparation of annual financial statements. A robust accounting framework facilitates timely and accurate reporting to internal stakeholders and external agencies. It is important to have adequate and effective controls in place in the accounting framework. The auditor shall focus on the control testing in the accounting framework. The auditor must assure himself that controls are in place and were effective during the entire audit period. Auditor must focus on following areas in the accounts maintenance and accounting framework:

- Segregation of duties in the accounts department
- Maker-checker check in the accounting process
- Timely and regular accounts reconciliations are prepared
- Effective process to investigate differences and subsequent follow-up
- Controls on advance accounts and suspense account
- Timely and regular reporting to senior management
- Quality and frequency of MIS reports produced by accounts department
- Preparation and maintenance of basic accounting documents to facilitate effective audit trail
- Effective and efficient use of IT tools to maintain accounts
- Use of proper accounting standards to maintain accounts
- Uniform accounting policies governed preferably by an up to date accounting manual
- Effective two-way communication between the spending units and accounting unit
- Transparency in accounts preparation
- Capacity of accounts staff

Risks	Tests to be performed
Accounting policies do not exist or/and are not updated in an accurate and timely manner (basis changes in regulatory requirements)	- Verify if documented accounting policies exist and have been duly approved. - Verify if a process exists to identify changes to accounting standards/guidelines and regulatory requirements on a periodic basis and updating the accounting policies accordingly. - Understand if all the updates made to the

Risks	Tests to be performed
	accounting policies and procedures are approved as per DoA before they get effective. - On a sample basis, test check whether documents are available to evidence review and approval of the updates made.
Changes to accounting policies and procedures are not communicated to concerned employees in a timely manner	- Understand the process of communicating the changes to the accounting policies and procedures to the concerned personnel. Understand the timelines for communicating such changes and how the list of concerned personnel is maintained. - Test check if the latest update to the accounting policy were communicated to the concerned employees within the defined timelines. - Understand if periodic training sessions are conducted to orient the concerned employees on accounting policies and procedures. Test check if such trainings have been conducted on a periodic basis. Also, test check for the last such training conducted, if it was attended by relevant personnel and conducted by authorised personnel.
Chart of Accounts (COA) is used inconsistently between business units	- Verify if there is a standard chart of accounts in operation, specifically, in respect of organization with multiple entities where accounts are consolidated at the group level. - Understand if the standardised chart of account has been communicated appropriately to all the concerned Accounting personnel in various business units.
Inaccurate set up or changes to account codes	- Understand the process of creation and modification of account codes. Review the approvals required for creation/modification of account codes. - For a sample of new account codes created / account codes modified during the audit period check whether the account code creation/modification form has been approved as per DoA. - For a sample of new account codes created/ account codes modified check the accuracy of account code details

Risks	Tests to be performed
	updated in the system with the approved account code creation/modification forms. - Review the system configuration to verify if all essential account code details are to be mandatorily entered into the system. - Review the system configuration to verify if there is maker checker applied on the account code creation/modification module. - Compare the COA with the financial statements (Trial balance) to identify account codes that are not included in the COA. - Test check for approvals for creation of the account codes identified above. Ascertain the reasons for non updation to the COA.
Unauthorized changes to the chart of accounts (COA)	- Obtain an understanding of the DoA matrix and process for granting, reviewing and removing system access rights for making changes to COA. - Verify that segregation of duties have been defined between the personnel responsible for updating COA and the personnel responsible for posting of journal entries. - Review whether system access rights to update the COA have been restricted to authorized personnel only. - Understand whether system maintains a log of changes made to COA and ascertain whether the log is reviewed periodically. - Obtain a sample of such reviewed logs and verify if the review was performed accurately and timely. - If such a log is not maintained, check that changes made to COA during the audit period have not been made by unauthorized personnel.
Duplicate/ Inactive Account code Exists	- Review system configuration to verify that system restricts creation of duplicate account codes. - Review the list of account codes to check for duplicate account codes (same code but different description or same description but different codes). - Understand if the organization has a process of periodic review of Chart Of

Risks	Tests to be performed
	Accounts to identify duplicate/redundant Account codes. - Understand the process of deactivation of account codes which are inactive for a defined period of time. - Review if system allows posting of journal entries on account codes made inactive in the system.
Events / transactions requiring an accounting entry are not posted in a timely manner	- Understand the process in place to identify journal entries not yet posted. Understand if there is a process of reviewing pending journal entries (parked but not posted). - For the audit period, verify if the list of pending journal entries was reviewed by authorized personnel. - If a review of pending journal entries is not performed, then perform analytics to ascertain ageing of pending journal entries.
Unauthorized posting of journal entries/ Journal entries are posted inaccurately	- Review the Accounting system to ascertain if the system enables the control of parking and posting of journal entries. - Obtain an understanding of the DoA matrix and process for granting, reviewing and removing system access rights for parking/ posting journal entries. - Verify that segregation of duties have been defined between the personnel responsible for parking of journal entries and the personnel responsible for posting of journal entries. - Review system access rights to verify if the access to park and post the journal entries has been restricted to authorised personnel only. - Check for journal entries if they have been parked and posted by the same individual. - For sample journal entries during the audit period, test check - It has been adequately reviewed before posting and authorised as per DoA - Required supporting documentation is available - The amounts have been calculated correctly - Journal entry has been posted to

Risks	Tests to be performed
	correct account codes - Journal entry has been posted in the correct accounting period - Review if the system has been configured to require that journal entries balance (debit and credit amounts match). - Review if the system restricts posting of entries only in the 'open period'. - For the audit period, review the number of adjustment entries posted. In case the number of adjustment entries is large, understand the reasons for the same. - For sample adjustment entries ascertain the reasons.
Duplicate journal entries are posted	- Review if the journal entries and batches are sequentially numbered by the IT system. - Verify if there is a process of review of significant account codes to assess the accuracy and reasonableness of the balances therein before the trial balance is finalised for monthly close. - For a sample such reviews, test check the supporting documents available evidencing the review. - Perform data analytics to identify duplicate journal entries.
Transaction data does not reconcile to the GL	- Verify if balance in sub-ledgers are posted automatically to general ledger accounts based on pre-defined grouping. - Understand the process and timelines for reconciliation of sub-ledgers to the GL. - For the audit period, obtain sample sub ledger reconciliations and review the following : - If the reconciliation was performed as per the defined timelines - If the reconciliations were reviewed and approved by the authorised personnel. - Reconciling items were appropriately and timely dealt with and resolved
Financial records are not retained as per the organization policy	- Verify the existence of a policy defining procedures for retention of various accounting and financial records. Understand if the record retention procedures defined in the company policy are based on the applicable regulatory requirements.

Risks	Tests to be performed
	- Test compliance with document retention policy for sample documents.
Financial records are accessed by unauthorised personnel.	- Review the physical access controls to the storage areas where financial and accounting records are stored (whether they are secured and locked, who has custody of the keys, etc) - Review whether access logs are reviewed on a periodic basis to ensure unauthorized access is prevented.
Book Close procedures are not adequately defined, communicated or adhered to.	- Obtain an understanding of the book closing procedures followed by the organization. Verify if the book closing procedures are documented and clearly communicated to the concerned employees. - Verify whether a book closure checklist defining the book close tasks, timelines and responsibilities exists. - Review completed book close checklists for a sample of months during the audit period. Test check : - Items included in the checklists were indicated as completed as per the timelines defined in checklist - All items were completed prior to final closing - Verify that the checklist was reviewed by authorised personnel before final book close - Appropriate evidence was documented for each completed task
Period-end adjustment journal entries are not correctly identified, calculated, and posted	- Verify if the book close checklist contains the list of usual adjustment journal entries posted at month end along with responsibilities for calculation, review and posting. - For sample period close journal entries test check whether they have been : - Adequately reviewed before posting and authorised as per DoA - Adequately supported with evidence - Calculated correctly - Posted to the correct account codes - Posted in the correct accounting period - Review if the adjustments are compared to prior period amounts. - For a sample of such entries, verify if the

Risks	Tests to be performed
	prior period amounts were reviewed. - Identify the journal entries posted after the book close cut-off date and test check if they have been posted in the correct accounting period.
Suspense/ Clearing accounts are not reviewed and reconciled before book close	- Understand the process of reviewing and reconciling suspense accounts for book close. - For sample months during the audit period, verify if suspense accounts were reviewed and cleared on the basis of adequate supporting.
Inaccurate/inadequate accruals, reserves or provisions	- Review if the list of accruals/ reserves/ provisions to be created for closing of books is mentioned in book close checklist. Check if the responsibility for calculation, review and approval of amounts is mentioned. - For the sample of key reserves and provisions, test check whether they have been : - Adequately reviewed before posting and authorised as per DoA - Adequately supported with evidence - Calculated correctly - Posted to the correct account codes - Posted in the correct accounting period - Obtain a sample of accrual journal entries and verify that these have been reversed in the corresponding accounting period.
Prepaid expenses are not amortized accurately on a timely basis	- Review if the list of pre-paid expenses to be amortised for closing of books is mentioned in book close checklist. Check if the responsibility for calculation, review and approval of amounts is mentioned. - For the sample of entries for amortisation of pre-paid expenses, test check whether they have been : - Adequately reviewed before posting and authorised as per DoA - Adequately supported with evidence - Calculated correctly - Posted to the correct account codes - Posted in the correct accounting period
Delay in closing of books of accounts.	- Verify if the book close timeline has been met consistently during the audit period. In case timelines were not met, ascertain reasons for the same and verify if any

Risks	Tests to be performed
	action plans were drawn. - Compute cycle time in days to perform monthly and annual close. Compare this with leading practices and identify areas of improvement.
Reconciliations not performed accurately and in a timely manner.	- Review if the list of reconciliations to be performed for closing of books is mentioned in book close checklist. Check if the responsibility for performing, review and approval of reconciliations is mentioned. - For the sample of reconciliations, test check whether: - Reconciliations have been adequately performed and authorised as per DoA - Reconciliations are supported with adequate evidence - Reconciling items have been correctly dealt with - Resulting adjustment entries have been posted to the correct account codes - Resulting adjustment entries have been posted in the correct accounting period
Journal entries booked or modified after the financial statements have been finalized/ close of accounting period.	- Verify if system is configured to prevent posting/modification of entries post the period close. - Obtain an understanding of the DoA matrix and process for granting, reviewing and removing system access rights to open/close accounting period in the IT system. - Verify that segregation of duties have been defined between the personnel responsible for opening/closing of accounting period and the personnel responsible for posting of journal entries. - Review system access rights to verify if the access to close / open accounting period in the IT system is restricted to authorized personnel only. - Understand whether system maintains a log of opening /closing of accounting period in the system and ascertain whether the log is reviewed periodically. - Obtain a sample of such reviewed logs and verify if the review was performed

Risks	Tests to be performed
	accurately and timely. - If such a log is not maintained check that opening /closing of accounting period in the system during the audit period has not been performed by unauthorized personnel. - Test check if prior periods for which book closure has been approved are closed in the system.
Absence of a process of recognition of liability for instances where goods/services are received but invoices are pending	- Understand process of creation of liability in instances where goods/services have been received, however invoices are pending Verify existence of GRIR/SRIR (temporary goods receipt account) accounts for these instances
Fraudulent invoices introduced into the system and being subsequently paid	- Assess the process to approval of invoices before they are finally processed for payment Check sample invoices for adequacy of management control to ensure that the goods and services being charged for have actually been fully received
Invoice processed even where the goods were either returned or proved to be unsatisfactory	- Identify instances of early payments (before the credit period) and match the same against material rejects, goods returned and/or services rejected
Duplicate invoices processed for payment or an invoice processed for payment more than once	- Establish system based/manual controls to prevent processing duplicate invoices or processing an invoice more than once
Invoice processed using cash route thus circumventing the system	- Understand the process to set up a new supplier and vendor into the ERP system before processing the invoice to ensure that payments are only made to valid and approved suppliers Review cash payments and identify instances of vendor invoices processed through that route
Long aged vendor advances and pending payments	- Review the vendor ledgers and establish instances of long pending advances and/or payments Discuss these with relevant process owners and establish reportable exceptions on premature or overdue payments

Cash/ Bank and Fund Management

Illustrative risks and control tests for cash/bank and fund management are as follows:

Risks	Tests to be performed
Ineffective/absence of segregation of duties for cash disbursements, receipts and accounting for cash	- Assess segregation of duties between cash application and cash deposit functions and identify overlaps
Unauthorized cash transactions	- Obtain cash book/register/ledger to validate if all cash transactions are updated in an accurate, complete and timely manner - Conduct a surprise verification of cash on hand and comment upon the adequacy of the process to perform this on an ongoing basis by an independent person in the organization
Inoperative bank accounts	- Identify inoperative bank accounts from the trial balance Discuss with the CFO the nature and need for these inoperative accounts
Bank accounts not reconciled	- Re-perform sample reconciliations to establish correctness of reconciliation - Verify if the bank reconciliation statement is reviewed and approved
Limits not defined for various bank signatories	- Review the approval/board resolution authorizing various cheque signatories - Check if all the signatories are still part of the organization
Weak monitoring controls over cheque books	- Understand the nature & quantum of cheque transactions and perform verification/reconciliation of stationary of cheque books - Ascertain whether Post Dated Cheque (PDCs) are received from customers and perform a verification/reconciliation of PDCs in hand
Cash flow forecast without the use of correct and authentic information	- Check the cash flow statements against the base data for accuracy and comprehensiveness Focus on aspects like: - borrowings & repayments are not recorded back; - surplus funds are not reported accurately; and - deposits made in excess of limits
Access to bank account information and ability to open, add, update, display, or correct such information not restricted	- Understand who has the password to operate bank accounts Establish how these password are updated, modified and safeguarded from any misuse
Unauthorized use of electronic fund transfer facility	- Review effectiveness of the process to authorize the wire transfer before a transaction is executed
Irrelevant fees and commissions charged by	- Critically review the bank statements and

Risks	Tests to be performed
the bank	identify commission, fees, interest charges which are not in line with the transactions executed

Hire to retire review (personnel review)

Hire to retire process covers the process from joining of employee to the retirement or detachment of employee. Key processes of the hire to retire cycle are as follows:

- Updates to employee master records
- Attendance and leave recording
- Payroll processing
- Payment of salaries
- Full and final payments

Auditors must perform controls for following risks associated with each of the above mentioned processes:

Risk	Tests to be performed
Updates to employee master records	
Unauthorized additions/modifications are made to employee master.	- Test check that employee master information has not been created /modified by individuals not authorized to do so. - For sample new employees added during the audit period, ascertain that approved employment contract exists and whether employee actually works with the organization. - Test check on a sample basis that employee master is updated only on the basis of approved documentation such as appointment letters, increment letters etc. - Reconcile number of employees as per the employee master vis-à-vis reported as per internal MIS.
Inaccurate data in the employee master	- Obtain the list of new hires and test check on a sample basis that details have been updated accurately in the employee master as per employment and salary contract. - For last annual salary change communicated to payroll department review whether this change was supported by approved communication. Test check individual line items to the employee master on a sample basis.
Delay in removal of separated employees	- For a sample of separated employees

Risk	Tests to be performed
from the employee master.	ascertain the date of resignation, last working day as per notice period calculation and date of leaving as per the employee master.
Delay in creating employee codes for the new joiners	- Understand the process and timelines for updating payroll master. - For a sample of recent recruitments, verify if the employee codes were created on a timely basis.
Attendance and leave recording	
Attendance recorded is inaccurate	- Compare the attendance recorded in the time keeping system with the attendance used for payroll processing and verify that there are no differences. - Verify that hours worked by employees as per the time keeping system do not exceed the maximum hours permitted as per the statutory laws.
Unauthorized modifications to the attendance data	- Obtain an understanding of the roles and responsibilities for updating and monitoring attendance register. - Review access rights over time-keeping records and verify that access has been granted to authorized individuals only. - Review physical access controls over attendance sheets. - For sample employees verify that employees had signed attendance sheets on a daily basis. Verify for distinct changes in signatures of same employee.
Payroll processing	
Inputs for payroll processing are not authorized	- Obtain the roles and responsibilities for the payroll team and verify that responsibilities have been segregated. - Review payroll computation for sample months and for sample employees verify that inputs for attendance, leaves and deductions for leave without pay have been computed accurately and are authorized as per the defined DoA matrix. - Reconcile monthly fixed salary elements in the employee master with the payroll file. - Reconcile bank account numbers in the employee master with the payroll file.
Payroll computation is not reviewed	- Verify that monthly payroll run is compared/ reconciled with previous month's payroll run to identify variances. - Understand how these variances are

Risk	Tests to be performed
	reviewed and analysed on a monthly basis.
Employee loans/ salary advances are not disbursed and recovered as per the policy	- Review the policy for employee loans and salary advances. - For a sample of employee loans/ salary advances disbursed during the audit period, test check : - Whether loans/ advances have been disbursed to employees as per the terms defined in the policy. - Whether approvals have been obtained as per the defined DoA matrix before disbursement of loans/ advances to employees - Loans/ advances are not due from separated employees - Obtain the list of pending employee advances and perform an ageing analysis to identify overdue advances. - Test check for sample employees that advances have been recovered as per the policy.
Payment of salaries	
Salary payments are not as per output of payroll processing	- Obtain an understanding of the process of disbursement of salaries to employees. Also, understand how the communication is sent to banks for payment of salaries. - Obtain the salary disbursement file for sample number of months and reconcile the total pay-out between salary disbursement file and payroll processing file.
Salary is paid to the wrong person.	- Obtain the salary disbursement file and verify that salaries are paid to employees existing in the employee master. - Obtain the salary disbursement file and verify that salaries are not paid to employees who have left the organization. - Verify that personnel in the Full and Final Settlement category are not included in the final salary pay-out for the month. - For salary payments made through manual cheques, test check on a sample basis that payments are made only through crossed cheques and no bearer cheques are issued. - For salary payments through manual cheques, test check on a sample basis

Risk	Tests to be performed
	that the employee signed for acknowledging receipt of cheque.
Full and final payment	
Full and final payments are based on unauthorized and inaccurate inputs	- Obtain an understanding of the procedures for processing full and final payments for separated employees. - For a sample of separated employees test check that clearances had been obtained from departments as per the defined policy prior to processing full and final payments. - Determine that procedures exist to monitor that assets are recovered from employees prior to exit from the organization. - For a sample of Full and Final payments processed, check if assets have been recovered. - Verify from the fixed assets records if there are any assets assigned to employees who have left the organization.
Inaccurate computation of full and final payments	- For a sample of separated employees test check that the full and final settlement was accurately processed. Verify that a final settlement form was documented and trace each line item to source documents (eg.- details of outstanding loans and advances, leave encashment, statutory deductions, payment for notice period etc.)
Final settlements are not processed timely	- Obtain an understanding of the timelines for processing full and final payments for separated employees. - Ascertain delays in paying final settlement amount by comparing the last date of employment and the payment date as per the bank statement. Also, ascertain root causes for the delays identified. - Obtain an understanding of the procedures for follow up on full and final recoverable from separated employees. Test check on a sample basis that follow-up was carried out for recovery of dues from separated employees.

Subsidy Management

One of the key objectives of the NRREP is to provide subsidy for promotion of renewable energy use. All technical components of NRREP are involved in disbursement of subsidy to various stakeholders for promotion of renewable energy use. The auditor must familiarize himself with the provisions of Subsidy Disbursement Mechanism of NRREP technical components before the audit execution. Auditor must conduct the following activities to review the subsidy disbursement process:

- Prepare a list of documents involved in the subsidy disbursement cycle. Check that such documents are adequately prepared at all levels.
- Identify key stakeholders and their responsibilities in the subsidy disbursement cycle e.g. implementing agencies, end user, private companies, regional service centres etc. Check that each stakeholders is effectively managing his responsibilities
- Identify the role of each stakeholder in the subsidy management and list the documents to be prepared and retained by each stakeholder. Check weather each stakeholder is maintaining and retaining the required documents or not.
- Familiarize himself with the quantum of subsidy that can be disbursed under different technical components
- Check the control documents for subsidy disbursement are properly prepared and reviewed e.g. subsidy calculation sheet
- Check that subsidy is provided to eligible end users
- Check that subsidy is provided as per the policy of NRREP

Risk	Tests to be performed
Adequate documentation is not maintained for subsidy disbursement	Check that subsidy disbursement records are maintained as per requirements of Subsidy Disbursement Mechanism
Correct amount of subsidy is not disbursed	Test check the subsidy calculation on sample basis as per subsidy disbursement policy
Subsidy is provided to ineligible end-users	Check subsidy disbursement documents and check that subsidy receivers fulfill criteria for subsidy benefit

4.2. Procurement Review

Scope

Audit of procurement is a regular process which is normally carried out after the completion of the fiscal year. As the process of procurement has to be conducted as per specified rules and regulations, its examination and evaluation of use of resources is a critical task. The main audit objective is to ensure that the procurement of goods and services have been done efficiently, economically, and effectively within the provision of the relevant guidelines such as Contract Agreement, Financial Procedure Act, Financial Administration Rules, Public Works Directives, Financial and Administrative Guidelines of NRREP and other relevant guidelines.

The scope of procurement audit must cover the following in respect of procurements:

1. Eligibility criteria
2. Pre-qualification of bidders
3. Validity of bids and bid security
4. Currency of bid
5. Time interval between invitation and submission of bids
6. Extension of validity of bids
7. Clarification and alteration of bids
8. Rejection of all bids
9. Negotiation
10. Award of contract
11. Scope of contract
12. Terms of payment
13. Advances
14. Prices adjustment
15. Duties and taxes
16. Transportation and insurance
17. Liquidated damages
18. Force majeure
19. Settlement of disputes
20. Foreign exchange fluctuations
21. Currency conversion

Coverage

Procurement review shall cover all the procurements carried out by the auditee during the last three years.

Bid management

Bid management is an important aspect of the procurement cycle and must be assessed to review the effectiveness of tendering process. Typical processes involved in bid management are as follows:

- Setting out the eligibility criteria for prospective bidders
- Assessing the pre-qualification of bidders
- Establish the validity criteria for bids
- Assess the bid security amount and collect bid security from bidders
- Preparation of advertisement for tender
- Preparation of scope of work
- Estimation of value of contract
- Receipt and custody of bids
- Opening and evaluation of bids
- Communication of evaluation result to bidders

Auditor must ensure that the above mentioned processes are managed as per the relevant provisions of Public Procurement Act and Public Procurement Regulations issued by Government of Nepal.

Contract management

Contract is awarded once the successful bidder is identified on the basis of submitted bids. Following the award of contract the contractor starts working on the project. Auditor must ensure that contract management is carried out as per the provisions of Public Procurement Act and Regulations to minimize the risk associated with service of contract. Auditor must ascertain the following:

- Contract is in writing and as per the standard mandated by PPA/ PPR
- Contract carries clear and detailed provisions related to dispute settlement, arbitration and terms of payment
- Contract must be signed by appropriate personnel
- Copy of contract is retained safely by the procurement staff
- Progress of work/ delivery of items is monitored and progress is reported to appropriate officers
- Any delay in contract delivery is identified by regular monitoring and brought to notice of contractor and officers through timely and written communication
- Contractors are paid on timely basis as per the progress of work and as per the provisions of contract

Value for money and price analysis

Value for Money (VfM) is defined as being ‘the optimal use of resources to achieve intended outcomes’. Value for money is not only about purchasing the cheapest alternative. Value for Money is about maximising the 3Es, so that maximum effectiveness, efficiency and economy can be achieved in procurement.

Economy: Are inputs of appropriate quality bought at the right price? (Inputs are things such as staff, consultant, raw material and capital goods that produce other outputs)

Efficiency: Efficiency refers to the fact that how well are the inputs converted into outputs? (Outputs are results delivered to an external party)

Effectiveness: Effectiveness is considered by assessing that how well the outputs were able to achieve the desired outcome.

While performing procurement review, auditor must check that value for money was considered while making the procurement or not. In this regard, auditor can also check that a price analysis was carried out by the purchaser or not. Price analysis refers to the check, that if purchased through the open market under standard conditions, how much money would the purchaser would pay for similar goods or service.

Auditor must comment on the value for money achieved during the procurement process and effectiveness of price analysis and its impact in getting the best price for goods and service. If the auditor is convinces that goods and services of same quality could have been procured for lesser price than such observation must be mentioned prominently in the audit report.

For the purpose of value for money review, the auditor shall refer to the Department for International Development's 'How to Note'. As per this document the good practice principles and benchmarks shall form basis for Value for Money reviews. These principles and benchmarks customized to the needs of the Compliance Unit and a particular audit, on the advice of the International Senior Compliance Advisor shall include review of benchmarks to determine existence of a framework in auditees to ensure the level of value for money achieved and measures required to achieve the gaps in existing and desired levels.

4.3. Performance review

Scope

Performance audit is an independent assessment or examination of the extent to which an entity, programme or organisation operates in terms of efficiency, effectiveness and economy.

As per the International Congress of the Supreme Audit Institutions (INTOSAI) auditing standards, Performance auditing embraces:

(a) Audit of the economy of administrative activities in accordance with sound administrative principles and practices and management policies;
(b) Audit of the efficiency of utilization of human, financial and other resources, including examination of information systems, performance measures and monitoring arrangements, procedures followed by audited entities for remedying identified deficiencies; and
(c) Audit of the effectiveness of performance in relation to achievement of the objectiveness of the audited entity, and audit of actual impact of activities compared with the intended impact.

The basis of performance auditing is the public accountability. Public accountability means that those in charge of a government program or ministry or fund are held responsible for the efficient and effective running of such responsibility. The two basic questions that performance auditor tries to answer are:

- Are things done in the right way?
- Are the right things are being done?

The key objective and benefits of conducting performance audit in a government are:

- Economy- keeping the cost low
- Efficiency- making the most of available resources
- Effectiveness- achieving the stipulated aims or objectives

Some of the key features of the performance audit include:

- Performance audit is flexible to select audit areas within its mandate
- Performance audit is not regular audit with formalized opinion. It is an independent examination on non-recurring basis.
- Performance audit is not a checklist-based audit
- Performance audit are generally ex post audits
- General aims of the legislature is taken for granted
- Professionalism and care are fundamental principle of conducting the performance audit

Coverage

Performance Audit is concerned with the evaluation of execution of NRREP implementation plan or any other activity of the NRREP and it embraces the following:

a. **Economy:** Audit of the economy of administrative activities in accordance with sound administrative principles, practices and Department policies.

b. **Efficiency**: Audit of the efficiency of utilisation of human, financial and other resources including examination of information systems, performance measures and monitoring arrangements and procedures followed by audited entities for remedying identified deficiencies.

c. **Effectiveness**: Audit of the effectiveness of performance in relation to the achievement of the objectives of the audited entity and audit of the actual impact of activities compared with the intended impact.

Objective

The basic objective of Performance Audit is to improve administration and accountability by way of:

- The quality of information and advice available to NRREP steering committee for the formulation of policy.
- The existence and effectiveness of administrative machinery to inform the NRREP steering committee whether programme objectives and targets have been determined with a view to fulfilling policy objective.
- Whether and to what extent, stated programme objectives have been met.
- The economy, efficiency, effectiveness, equity and ethics of the means used to implement the programme / activity.
- The intended and unintended, direct and indirect other impacts of programmes / activities; for example, the environmental impact of NRREP activity etc. and
- Compliance to applicable laws and regulations in the context of Performance Audit objectives.

Guidance for performance audit

The basic principles of Performance Audit may be outlined as under:

- Performance Audit is an assessment of efficiency and effectiveness of the programmes, with due regard to economy;
- Apart from the question whether the things are being done the right way, it also addresses the question of whether the right things are being done, in other words, it also focuses on what is not being done rather than only on what is being done;
- Performance Audit is undertaken with the objective to improving performance of public sector programme and, therefore, an assessment of the expected impact-qualitative and quantitative – on the programme must be made before undertaking the audit;
- The subjects selected for Performance Audit could be a programme, segments of a programme – including the processes, procedures and systems, and entity itself or parts of an entity etc.;
- The subject of Performance Audit could be financial, non-financial or public interest and governance issues;
- While the Performance Audit may and shall assess the implementation of the policy through one or more programmes, the scope of audit shall be limited to assessing and impact of the implementation of policy and the policy per se shall not be questioned;
- Performance Audit shall be conducted in time, when there is scope for remedial.

The IA team shall study the following documents/ papers/ reports etc., which will help in conducting a meaningful Performance Audit:

a. Plan, budget documents, vision/mission statements and strategic plan of the entity to be audited
b. Enabling legislation
c. Entity organisational chart, programme execution format and accountability relationship
d. Annual reports, performance budget and accounts, etc.
e. Programme documents containing the parameters of the programme notes and minutes etc.
f. Programme guidelines issued by the entity, administrative and implementation instructions, information feedback / monitoring reports and action thereon and minutes of the meetings on relevant subject, etc.
g. Administrative and technical inspection reports within the entity, proceedings of the monitoring meeting, internal audit reports etc.
h. Evaluation reports and surveys sponsored by the entity, independent evaluations and survey; publications/reports by other agencies on the subject.
i. Past audit reports of financial/ regularity or Performance Audit and their follow-up.

Planning and preparation before performance audit

Developing measurable objectives/ performance indicators: The responsibility for the development of measurable objectives and performance indicators as also the system of measurement rests with NRREP Compliance Unit. Compliance Unit is also required to define immediate and final outputs and outcomes in measurable and monitorable terms. Internal audit team shall discuss these issues with the Compliance Unit before commencing Performance Audit.

Interaction with the entity: Performance Audit envisages a high degree of interaction with the auditee, right from the selection of subject(s) through the actual process of Performance Audit, developing and finalizing the Performance Audit report.

Understanding the subject: The first step in planning the individual Performance Audit is to develop a sound understanding of the subject of audit. Such understanding will help in identifying the key audit issues.

Comptroller Auditor General of India has one of the leading performance audit guidelines and shall be followed for performance audit. The internal audit team shall observe the Performance Audit Guidelines lay down by Comptroller Auditor General of India (CAG) to conduct performance audit as listed below:

1. Information on the programme/ subject of audit as given below:
    a. Programme inputs/ outputs
    b. Programme process and resource flow chart with explanatory note.
    c. Execution structure or institutional design.
    d. Expected cost-benefit/ input-output as per the programme design.
    e. Programme beneficiaries.
    f. Performance measures if any set in the programme.
    g. Expected programme objectives and impacts.
2. Scope of Performance Audit in terms of period of operations to be audited, segment or activities or entities to be audited, etc.
3. Criteria to assess if the programme objectives fulfill the policy objectives.
4. Basis for comparison of the intended impact with the actual impact.
5. Programme evaluation techniques to be used in the Performance Audit.
6. Impact evaluation, if possible on the basis of available evidence i.e. whether the observed impacts are attributed to the programme or there are other reasons also.
7. Audit evidence including their type i.e. primary and secondary corroborative evidence under the categories of documentary, physical, oral or analytical, source and evidence gathering techniques such as direct observation, survey, photographs, interviews, etc.
8. Expected value addition to the programme through Performance Audit.
9. Expert or consultancy services/ outsourcing if required.
10. Evaluation of internal control system.
11. Risk analysis and Sampling Techniques.
12. Recommendations development process and test of recommendations on the internal control parameters;

13. Report writing procedures.
14. Series of actions/steps expected at each stage for entity involvement.
15. Entry and Exit Conferences and minutes thereof.
16. Periodic reporting, Report approval, printing and presentation to HOD / Secretary concerned.

Performance audit guidelines can be referred to by visiting http://www.cag.gov.in/html/publi_peraudguid-rc.htm

4.4. Regulatory review

Scope

Regulatory compliance describes the goal that corporations or public agencies aspire to achieve in their efforts to ensure that personnel are aware of and take steps to comply with relevant laws and regulations. The scope of regulatory compliance must cover the compliance to acts and regulations of Nepal listed in the 'List of regulations' section.

Coverage

The objective of compliance review is to ensure that all regulatory and statutory provisions relevant to NRREP are followed. Regulatory review must review the compliance to applicable regulations during the audit period.

Illustrative list of regulations

1. Banks and financial institutions regulations by Nepal Rastra Bank
2. Banks and financial institutions act, 2063 (2006)
3. Financial Procedures Act, 2055 (1999)
4. Financial Procedure Rules
5. Local Body Financial Administration Rules, 2064 (2007)
6. The Public Procurement Act, 2063 (2007)
7. The Public Procurement Rules, 2064 (2007)
8. Audit Act, 2048 (1991)

The above mentioned regulations are illustrative. An exhaustive list of applicable regulations must be prepared by the audit team in consultation with auditee and Compliance Unit. Such applicable regulations may vary from one auditee to another.

Regulatory review focuses on the compliance to regulatory provisions of various statutes applicable to the entity. The preferred method for such review is to prepare self-assessment questionnaires on the basis of mandatory regulations identified by audit team in consultation with auditee and compliance unit. Such self-assessment questionnaires must be filled up by the auditee and correctness of response shall be checked on sample basis by the review team. An illustrative list of control tests is given below:

Control Objectives & Activities	Test Steps
1) Entity level objectives are established, documented and communicated.	
1.1 Management has a business planning process in place which examines existing objectives and established new objectives when necessary.	1. Interview strategic management to understand the process followed to set objectives in the auditee. Obtain documents and verify whether: - there is involvement of all levels of management in objective setting; - entity-wide objectives were established; - objectives were established for each significant activity; - related objectives support strategic objectives; - objectives are reviewed periodically, and if this activity is documented; - external and internal factors were assessed prior to objective setting.
1.2 Management establishes business plans and budgets with realistic goals, and incentives for achievement of plans are balanced with an emphasis on accurate reporting.	1. Interview management and determine the methods used to prevent unauthorized investments. 2. Perform testing to ensure unauthorized access is prevented by comparing the list of approved personnel who can invest and with the access granted.
1.3 Objectives are communicated to the appropriate levels, and are understood and adopted by the responsible parties.	1. Interview strategic management and verify that: - information on the entity-wide objectives was disseminated to employees and the Board of directors; - management obtained feedback from key managers, other employees and the Board signifying that communication to employees is effective.
1.4 The entity has a process in place to periodically review and update entity wide strategic plans and objectives.	1. Interview strategic management and verify on how often plans and objectives are being reviewed and updated. 2. Obtain and verify the plans and objectives to ensure that they are being reviewed and updated.
2) Management has established practices for identification of risks.	

Control Objectives & Activities	Test Steps
2.1 Management has forward-looking mechanisms to provide early warning of potential risks relevant to the preparation of the financial statements.	1. Interview management about the process followed by the auditee to be aware of potential risks relevant to the preparation of the financial statements. 2. Verify if the auditee has classified such potential risks in the following series of assertions: existence or occurrence, completeness, rights and obligations, valuation or allocation, presentation and disclosure. 3. Evaluate the ERM Framework adopted by the entity.
2.2 Risks considered include risks arising from both internal and external events.	1. Interview management regarding the process followed by the auditee for the event identification (considering either events with positive impact, and the events with negative impact). Verify if this task was documented. 2. Ensure that during their risk identification process, the auditee considered internal and external events; look at the following examples: - External Factors: supply sources, technology changes, creditor's demands, competitor's actions, economic conditions, political conditions, regulation, natural events. Internal Factors: - human resources - such as retention of key management personnel or changes in responsibilities that can affect the ability to function effectively. - financing - such as availability of funds for new initiatives or continuation of key programs; - labor relations - such as compensation and benefit program to keep the entity competitive with others in the industry; - information systems - such as the

Control Objectives & Activities	Test Steps
	adequacy of back-up systems in the event of failure of systems that could significantly affect operations. 3. Also, consider evaluating the ERM Framework adopted by the entity.
2.3 Management identifies risks related to each of the objectives established.	1. Use information obtained above at 1.1 regarding objective setting. Interview management to understand how the auditee identifies risks related to each one of the objectives established. 2. Obtain and verify the auditee uses a formal event identification technique (examples of names of these techniques are: event inventories; internal analysis; escalation or threshold triggers; facilitated workshops and interviews; process flow analysis; leading event indicators; loss event data methodologies). Also, verify if risks identified were documented. 3. Evaluate the ERM Framework adopted by the entity.
2.4 Management identifies financial reporting risks which result from operations and/or compliance with laws and regulations; e.g. business strategy and plans.	1. As established in 4.3 at "Control Environment" section, even if the auditee is not public, interview management to understand how the auditee has documented its Internal Control over Financial Reporting. 2. Obtain and ensure that the Internal Control over Financial Reporting is documented in accordance with the management intention.
2.5 Management identifies fraud risk factors; including management override of controls.	1. Interview management to understand how the auditee considers risks that may lead to fraud. 2. Verify whether anti-fraud programs are implemented inside the auditee.

Control Objectives & Activities	Test Steps
	3. Verify whether risk identification includes fraud factors.
2.6 Management identifies risks relating to non-routine transactions.	1. Interview the strategic management to determine if the risk identification process includes non-routine transactions. 2. Obtain documentation and ensure that the process includes non-routine transactions. Otherwise, assess the reasonableness for not including them.
2.7 Identifying risks includes estimating the significance of the risks identified, assessing the likelihood of the risks occurring, and determining the need for action.	1. Obtain evidence and verify whether the: - risks are analyzed through formal processes or informal day-to-day management activities; - the identified risks are relevant to the corresponding activity objective; - appropriate levels of management are involved in analyzing the risks. - a risk rating criteria exists.
2.8 Risks are evaluated as part of the business planning process.	1. Interview management and understand how periodically risk assessments are conducted, and if these are part of the business planning process. 2. Obtain and ensure that there is adequate evidence available to ensure that the risk assessments are conducted.
2.9 Risks are documented and communicated throughout the organization, as appropriate.	1. As mentioned above at 2.3, verify if risks identified were documented (i.e. risk matrices). Investigate how risks are communicated throughout the auditee. 2. Obtain corroborative evidence such as emails etc., to ensure that risk is communicated to appropriate personnel.

Control Objectives & Activities	Test Steps
2.10 The responsibilities and expectations for the entity's business activities and the entity's philosophy about identification and acceptance of business risk are clearly communicated to the executives in charge of those functions.	1. Interview management on how risk acceptance and tolerance is established in the entity. 2. Obtain documentary evidence and verify whether these were clearly communicated to the executives in charge of business activities.
3) Management consider the entire organization as well as its extended relationships in its risk assessment process.	
3.1 Internal audit (or another group within the auditee) identifies and updates all significant relationships, from variable-interest entities, outsourced service providers, significant suppliers and customers, to guarantors and guarantees of indebtedness. Such listing is reviewed by senior management on a regular basis.	1. Interview management, or the Internal Audit ors to understand how often external and internal factors are considered in the risk assessment process are evaluated and updated. 2. Verify whether management has assessed the relationship between such factors and have evaluated / updated the risk assessment periodically.
3.2 Financial reporting, regulatory compliance and operational objectives are set for each significant relationship or portfolio of relationships. From such objectives, a detailed risk assessment is performed.	1. ERM requires that risk be considered from an entity-wide, or portfolio, perspective. Interview management to understand the portfolio of relationships considered in the risk assessment process. 2. Verify that financial, regulatory and operational objectives were developed for each significant relationship, and that a detailed risk assessment was performed taking into consideration such objectives. 3. Evaluate the ERM Framework adopted by the entity.
3.3 Risk assessment of significant relationships and portfolio of relationships considers fraud, going concern, internal and external reporting, and accounting in accordance with GAAP.	1. With the information obtained above at 3.2, verify that risk assessment process considered fraud, going concern matters, internal and external reporting, and accounting in accordance with GAAP's (either local and international) which is periodically reviewed by management.

Control Objectives & Activities	Test Steps
3.4 There is documented oversight over the entire life-cycle of significant relationships, from initiation, continuing monitoring, and termination.	1. Interview management on all significant relationships (business units, departments, functions) involved in the risk assessment process. 2. Verify if such relationships are documented over its entire life-cycle, from initiation, continuing monitoring, and termination.
4) Management has implemented mechanisms to anticipate, identify, and react to changes.	
4.1 The business planning process includes a broad spectrum of personnel with collective knowledge of all areas of the entity.	1. Select 10 employees from different areas of the entity and obtain their background information from Human Resources (you may use the same sample chosen at 2.3 in section "Control Environment"). 2. Verify all the documents that support their background and experience and also determine if such background and experience is enough so the employee can perform the duties in his/her actual position.
4.2 The business planning process includes consideration of changes in the business environment including the industry, competitors, the regulatory environment, and consumers.	1. Interview management on the risk assessment techniques used in the auditee. 2. Verify whether such risk assessment techniques includes adequate consideration of changes in the industry, competitors, regulatory environment.
4.3 Changes in risks are identified on a timely basis; e.g. direct impacts such as new GAAP, non-routine transactions, or IT systems; or indirect impacts from events such as rapid growth, new products, supply sources, competition, expanded foreign operations, corporate restructurings, etc.	1. Interview management and investigate how often the event identification process takes place. Verify if this task is documented.
4.4 Changes are appropriately communicated to the proper of level of management (depending on the significance).	1. Interview management and determine what are the channels of communication used to disseminate changes in the business strategy, and to which

Control Objectives & Activities	Test Steps
	employees are these communications addressed.
4.5 Risk and opportunities related to changes are addressed at sufficiently high levels in the organization.	1. Interview management. Investigate if they are included in the communications sent by the Board regarding significant changes in the business strategy. 2. Obtain and verify that the organization has established a risk response to such new changes (verify written documentation if possible).
4.6 In order to ensure a comprehensive assessment of the auditee and its environment, management demonstrates a willingness to explore possibilities that they initially disagree with.	1. Interview a member of the Board (if possible) regarding their willingness to work in topics that they originally disagree with. Ask for an example (if any) and ensure that the same is documented as part of the Board minutes.
4.7 The business planning and risk assessment processes is completed at a sufficiently detailed level for the size and complexity of the entity.	1. Interview management on the scope of the risk assessment process. Understand how the areas/departments under the scope were selected to be included. 2. Obtain and verify the scope of risk assessment and ensure that the established procedure is followed.
4.8 In an effort to heighten awareness of risks and changes affecting the entity, management communicates the results of their risk assessment and changes in their business environment to all necessary employees.	1. Interview management to determine the channels used to communicate the results of the risk assessment throughout the entity. 2. Obtain and ensure that the management communicated the results if their risk assessment and changes to all the necessary employees.

Control Objectives & Activities	Test Steps
4.9 The auditee assesses the implications of acquisitions and divestures of significant businesses or assets.	1. Interview management on how the decision of acquisition/divestitures of significant business or assets is assessed within the risk assessment process. 2. Select and the verify acquisition/divestitures to ensure that the implications assessed appropriately.
4.10 Management has identified the resources needed to achieve the objectives and has plans to acquire the necessary resources, when needed.	1. Obtain evidence from the management about the most recent acquisition of significant resources (assets, business units, etc.) and determine if such acquisitions were made in order to achieve strategic or related objectives as intended by management.
4.11 Budgets and forecasts are updated during the year to reflect changing conditions.	1. Determine how often budgets and forecasts are updated throughout the year. 2. Obtain all the updated budgets and forecast prepared in the last two years, and assess the reasonableness of the period in which they were updated and the authorization to the budgets/forecasts.
5) Management evaluates and mitigates risks appropriately.	
5.1 Internal audit (or another group within the auditee) performs a periodic risk assessment, which is reviewed by senior management.	1. Interview management and obtain the evidence of review by senior management of the last risk assessment performed in the entity.
5.2 Senior management develops plans to mitigate significant identified risks and presents their findings and plans to the Audit Committee of the Board of Directors.	1. Interview management and understand what is the most common entity's orientation to risk response (avoid, reduce, share or accept). 2. Obtain the plan that was created for the identified risks to be reduced, shared or accepted. Verify if such plan is documented (i.e. risk matrices). 3. Verify evidence of discussion and

Control Objectives & Activities	Test Steps
	review of such plans with the Audit Committee.
5.3 Management and the Board receive periodic reports on identified significant risks and the results of actions taken to address them.	1. Interview management and a member of the Board (if possible) and understand how often they receive suggestions of risks that needs to be added to the risk assessment plan. 2. Ensure that there is an appropriate established channel in the entity so the Board can receive these kinds of suggestions.
5.4 Risks are reviewed periodically with the appropriate corporate governance functions; e.g. executive management, disclosure committee, audit committee, legal, etc.	1. Interview management and investigate how often the risk assessment plan is reviewed with the appropriate corporate governance functions and/or executive management. 2. Evaluate communication with executive management regarding the risk assessment.
5.5 When risks are identified, existing controls are examined to determine if there is a failure in controls and if so, determine the reason for such failure.	1. Interview management to understand the plan used to test controls that are designed to mitigate identified risks. 2. Obtain evidence and verify that the results of test of controls are communicated and specifically, senior management are aware of the controls that fail. Determine if remediation plans are implemented for control failures.
5.6 Management has specific programs or procedures in place to address and track fraud risk factors and fraud risks identified.	1. Interview management to understand how the auditee considers risks that may lead to fraud. 2. Obtain anti-fraud programs and ensure that anti-fraud programs are implemented inside the auditee (use the information obtained above at 2.5).

Control Objectives & Activities	Test Steps
5.7 The disclosure committee reviews risks identified as part of the assessment of the adequacy of the auditee's disclosures.	1. Interview a member of the disclosure committee (if it exists), understand how this committee reviews the identified risks, and how they select the most important risks that needs to be disclosed. 2. Obtain evidence and verify that the disclosure committee reviews the risk identified as part of auditee's disclosure.
6) Accounting principles are properly applied in preparation of the financial statements.	
6.1 A process within the accounting department exists to identify and address changes in GAAP made by relevant authoritative bodies.	1. Interview the CFO (or delegate) and understand the process to identify and address changes in GAAP (i.e. some companies have free subscriptions to accounting updates, like the service provided by Deloitte). Also, verify evidence that the accounting updates are disseminated within the accounting and finance areas.
6.2 The entity should have all significant accounting policies documented and changes to those policies must be approved by senior management and subject to review by the Audit Committee.	1. Interview the CFO (or delegate) and ask for all the significant accounting policies. If they don't exist, verify if informal guidelines were issued. 2. Verify whether such accounting policies were properly approved (by senior management and Audit Committee).
6.3 Changes in the entity's business practices that may affect the method or process of recording transactions and the proper application of GAAP are communicated to the accounting department.	1. Interview management and verify whether appropriate channels exist to communicate all changes in the entity's business practices that may have a financial impact and/or affect the actual method or process of recording transactions.

Control Objectives & Activities	Test Steps
6.4 Management works with independent auditors and other third party experts to appropriately address complex changes in GAAP.	1. Interview the Chief of Accounts (or delegate) and understand how the finance and accounting departments work with third parties in order to get a better comprehension of accounting and tax topics that may not be clear for them. 2. Verify if such communications with third parties is documented.
6.5 Management maintains current knowledge of GAAP issues and pronouncements.	1. Use the information obtained above at 6.1 to ensure that the accounting updates are disseminated within senior/executive management.

The Compliance Unit shall also review the compliances to the prevalent and applicable laws & regulations by the auditees so as to ensure that there are no risks of defaults or any such defaults are well justified with proper records and reasons for default. For this purpose, checklists of applicable clauses of the laws and compliances therein shall be prepared by the National Compliance Advisor for approval from the International Senior Compliance Advisor and implementation in audits / reviews by the auditors. The National Compliance Advisor shall be responsible for the periodic updation of this checklist.

5. Management Information System

5.1. Purpose

The purpose of Management information system (MIS) reports is to provide information to Steering Committee through lead donor in respect of status of compliance reviews and status of actions taken on audit observations identified in the audit reports.

5.2. Reporting requirements

Compliance unit is required to report to Steering Committee through the lead donor in respect of key performance parameters of Compliance unit. MIS reports are to be submitted to Steering Committee by the International Senior Compliance Advisor on quarterly and annual basis. The ISCA may also provide the MIS reporting to the Steering Committee on need basis if required.

5.3. MIS including action taken matrix

MIS report submitted by Compliance Unit must have status of audits scheduled to be completed during the year as per the annual plan. Steering Committee shall be informed about the number of reviews completed out of the total number of reviews to be conducted during the year. Ongoing audits, together with audits not started till date (delayed) must also be reported to the steering Committee in the MIS. Reasons for delay in commencement of audit must be communicated to steering Committee with action taken or desired to be taken to resolve the reasons for delay or non-start of audits. If for any reasons, the audits planned cannot be started, should be rescheduled for next periods and the Audit Plan should be updated accordingly.

Status of audit objections must be communicated to Steering committee. Actions taken and corresponding reduction in audit objections must be highlighted in the audit report and MIS with reasons for non-compliances. Key actions taken on audit observations must be highlighted in the MIS to be submitted to Steering committee.

5.4. Formats

The format of MIS reporting is given below. This table is illustrative in nature and can be modified on annual basis with the approval of ISCA and Steering Committee. The need for amendment in the format shall be assessed by the National Senior Compliance Advisor who shall submit the recommendation for change to ISCA for review and obtaining approval from the Steering Committee.

<table>
<tr><th colspan="5">Compliance Unit – MIS</th></tr>
<tr><td colspan="5">Date:
Period:</td></tr>
<tr><td colspan="5"><b>Status of compliance reviews</b></td></tr>
<tr><td>Review</td><td>Completed</td><td>Ongoing</td><td>Not initiated (with reasons and action taken to re-plan)</td><td>Rescheduling in case of audits not initiated</td></tr>
</table>

Compliance Unit – MIS				
Financial				
Performance				
Procurement				
Regulatory				

Status of audit objections									
Review	Opening (NPR)	Opening (Number)	Additions (NPR)	Additions (Number)	Cleared (NPR)	Cleared (Number)	Closing (NPR)	Closing (Number)	Reasons for pendency
Financial									
Performance									
Procurement									
Regulatory									

Status of quality assurance	
Peer reviews conducted: Key findings of peer reviews:	
List of review reports submitted to Steering committee during the financial year: 1. 2. 3.	
Instances of audit report not been submitted on time 1. *Audit report title – delay in number of days - reason* 2. 3.	

Action taken matrix				
Audit Title	Observation	Action taken	Impact	

5.5. Risk universe database

Risk universe database is a collation of risks identified during the reviews conducted throughout the year. Risk universe is compiled to facilitate aggregation of risks identified in different reviews. Risk universe provides an indication of the emerging risks across various components. An illustrative format of the risk summary table is provided below:

Risk Summary Table					
S. No.	Risk title	Description	Component	Risk area	

An operational area wise Risk Register shall also be maintained by the Compliance Unit. Each of these Risk Registers shall also contain risks compiled audit entity wise. The Summary of these Risk Registers shall be compiled in the table above. An illustrative format of the Risk Register is given below:

Risk Register – Operational Area …………..

Business Cycle :
Business Cycle Unit :
Risk Owner :
Entity :

Risk Identification *						Mitigation Measure narrative	Risk Polarization *			
Threat		Vulnerability		Risk						
No.	Description	No.	Vulnerability	No.	Description		Probability @	Impact @	Risk Score ^	Risk Classification+
T 1	xxx	V 1.1	xxxxxx	R 1.1.1	xxxxxx		High	Medium	30	High
Illustrative										
T 2		V 2.1		R 2.1.1						
				R 2.1.2						

Risk Identification *						Mitigation Measure narrative	Risk Polarization *			
Threat		Vulnerability		Risk						
No.	Description	No.	Vulnerability	No.	Description		Probability @	Impact @	Risk Score ^	Risk Classification+
				R 2.1.3						
				R 2.1.4						
				R 2.1.5						

Risk polarization may be done on basis of the following illustrative parameters:

Probability * $			Impact * #							
Does it have potential of occurring several times	Does it have possibility of occurring once or twice	Has it rarely occurred or is unlikely to occur in future	Accounting	Operational	Reputational	Regulatory	Budgeting	Procurement	Others (as may be decided)	Total Impact

@ Is the classification in High Medium and Low based on scores of individual scores of parameters for the category (i.e. Probability and Impact) based on macro enabled excel based working

^ Is summation of macro enabled excel working for scores allocated for each of the parameters for Probability and Impact

+ Is summation of Rating in High Medium and Low based on the overall score and rating of Probability and impact

** Illustrative parameters*

$ May be classified as Yes and No

# May be classified as High, Medium and Low

6. Quality Assurance

Quality is an essential or distinctive characteristic, property and attribute of a process. It is the degree to which a set of inherent characteristics of a product fulfils its requirement. Quality assurance or QA is a process through which the Compliance Unit shall assess and monitor the system of quality control and adherence through review of audit engagements.

6.1. Quality assurance framework

Quality should be embedded into each stage of the internal audit process. Quality appraisal is an assessment of how well internal audit has performed against its objectives. To establish whether the needs of the stakeholders were met and to identify areas for improvement, the following should be performed:

- Conduct ongoing evaluations against pre-established performance metrics
- Conduct periodic quality assurance reviews on the internal audit function

The following parameters shall form basis of quality assurance framework and assessment:

Scope: (i) Did the audit plan properly address all issues needed for successful and effective audit; (ii) Did the execution satisfactorily complete all the needed elements of the plan.

Reliability: Are the audit findings and conclusions truly reflecting actual conditions for areas examined.

Objectivity: Was the audit carried out in impartial and fair manner.

Timeliness: Were the audit results delivered at appropriate times.

Clarity: Was the audit reports clear and concise in presenting the results of the audit.

Significance: How important are the matters examined in audit in terms of their importance, risks and priority.

Efficiency: Were the resources, timelines and efforts commensurate to the size and complexity of the engagement and auditee.

Effectiveness: Did the findings, conclusions and recommendations get appropriate response from auditees and other stakeholders.

The above parameters may be reviewed by the Compliance Unit annually for inclusion and exclusions of parameters after each assessment of results of overall audits conducted in that year.

6.2. Policies and guidelines

Quality assurance shall be done for all reviews done during the year. Performance quality is critical to adding value. The audit team should work with the Compliance Unit to establish metrics that will be used to measure the team's performance. This will enable:

- The audit team to proactively drive the performance of internal audit activities
- Demonstrate to Auditee, Compliance Unit and the Steering Committee how internal audit has delivered value
- Identify areas of focus for future development and improved delivery

Developing performance metrics

Metrics should be specific, measurable and reasonable. The table below sets out number typical standard metrics:

Infrastructure
▶ Number of audits scheduled ▶ Number of audits completed ▶ Audit efficiency (Budget versus actual) ▶ Opportunities for cost reduction identified
Planning
▶ Timeliness of audit notifications ▶ Annual risk assessment planning efficiency
Fieldwork
▶ Average time spent in field ▶ Average cost per audit ▶ Percentage of audits that leveraged data analytics ▶ Number of leading practices identified and communicated
Reporting and communications
▶ Average number of days to issue final report ▶ Average report cycle time ▶ Percentage of reports with disputes and disagreement ▶ Percentage of recommendations implemented ▶ Percentage of issues past due ▶ Stakeholders satisfaction rating

6.3. Frequency and responsibility

Quality assurance is to be conducted by the Compliance Unit for all audits within 30 days of the submission of final audit report. A summary of the QA reviews shall be compiled on quarterly and annual basis and reported to Steering Committee. The summary shall also provide basis to ISCA to further improve the auditing function in NRREP and selection and re-appointment of auditors.

6.4. Quality assurance assessment

The following activities should be undertaken for Internal Quality Assessment:

- Perform Quality Assurance Reviews
- Develop action plans to address all key points raised in the review
- Link quality assurance review outcomes to individual performance appraisals, objectives and training plans

Quality reviews should be undertaken to assess that internal audit methodology have been appropriately applied to all stages of the internal audit process. Quality review of selected assignments should be performed by someone outside the engagement team. Preferably, it should be performed by ISCA or NCA.

The program should also assess the efficiency and effectiveness of internal audit and identify opportunities for improvement. The results of the quality assurance and improvement program should be communicated to the steering committee through the lead donor.

6.5. Quality assurance methods

QA reviews by the Compliance Unit shall be based on following methods:

- Compliance with **Quality control techniques** framed by Compliance Unit from time to time according to the needs of the audit and entity being audit at the time of instructions being issued to auditors and adopted by the auditors appropriate to circumstances under which an audit is planned to be executed and is conducted.
- Conduct of **pre-issuance reviews** before the audit report is formally issued to ensure that audit complies with the audit methodologies appropriate to an audit engagement and as were agreed upon
- Conduct of **post-audit reviews** after the conclusion of audits to ensure that shortcomings and areas of improvement are identified for adoption in next audits

6.6. References

The Compliance Unit shall refer to the Quality Assurance and Quality Control Standards issued by IFAC, INTOSAI and OAG, Nepal from time to time for appropriate adoption

7. Capacity Development

7.1. Objective

Capacity development may be defined as the process through which individuals, organisations, and societies obtain, strengthen, and maintain the capabilities to set and achieve their own development objectives over time. Compliance Unit is entrusted with the task of capacity building at entity and individual level in order to strengthen the capabilities of entities working in the renewable energy sector which are directly related to NRREP.

Key elements of capacity development are as follows:

- Capacity development is a process of change, and hence is about managing transformations. People's capacities and institutional capacity and a society's capacity change over time. A focus on what development policies and investments work best to strengthen the abilities, networks, skills and knowledge base cannot be a one-off intervention.

- There can be short term results. And often in crises and post conflict situations there is a need for such. But even short term capacity gains, such as increase in monetary incentives or introducing a new information system, must be supported by a sustained resource and commitment to yield longer term results that truly impact on existing capacities.

- Capacity development takes place at three different levels: the individual level, the organizational level and the societal level. These three levels are interlinked and interdependent. An investment in capacity development must design and account for impact at these multiple levels.

- Capacity development is about who and how and where the decisions are made, management takes place, services are delivered and results are monitored and evaluated. It is primarily an endogenous process, and whilst supported and facilitated by the international development community, it cannot be owned or driven from the outside. At the end of the day, it is about capable and transformational states, which enable capable and resilient societies to achieve their own development objectives over time.

As mentioned above, capacity development can be on following three levels:

The individual level - Individuals, as the tissues of organisations and societies, represent the first layer of capacity. For societies and organisations to transform and grow, they need individuals with skills, knowledge and experience. At the individual level capacity development takes place through demand-driven processes of learning and knowledge acquisition and sharing, experiencing, participation in communities of practice, south-south learning initiatives, on-the-job training, mentoring and coaching and other learning techniques that empower and place the individual in a central and active position. This new approach to capacity development moves away from the traditional technical assistance, mostly based on supply-driven technical training and workshops.

The organisational/institutional level - The second layer of capacity is the organisational or institutional level. As individuals make up the tissues of organisations and institutions, the sharing of skills, knowledge, experience and values amongst individuals belonging to a group or organisation translates, over time, into the very organisation's capacity, consisting of procedures, systems, policies and culture. However, while the collective set of capacities of individuals ultimately translates into the organisational and institutional capacity, the latter by far exceeds the sum of the capacities of their members. Developing organisations' or institutions' capacity means fostering change within their complex system of policies, systems, procedures, regulations and organisational culture; a process, the latter, which is endogenous and voluntary, fully owned and controlled by the organisations and institutions that are undertaking change.

The societal level - The third layer at which capacity development takes place is the societal level. Transformation and change that happens at the societal level overhauls and, at the same time, is driven by that which takes place within individuals and organisations that make that society. In turn, the values system of a society, its customs, body of laws and policies, the system of governance are all elements that impinge on the ability of individuals and organisations to develop further their capacity and transform. Change in capacity at the societal level is a long process, which is difficult to control and steer; however, it is not to be considered an externality or a variable that cannot be controlled for. Through capacity development at individual and entity level, Compliance Unit shall indirectly contribute to societal level capacity development.

7.2. Needs assessment

A needs assessment is a systematic process for determining and addressing needs, or "gaps" between current conditions and desired conditions or "wants". The discrepancy between the current condition and wanted condition must be measured to appropriately identify the need. The need can be a desire to improve current performance or to correct a deficiency.

Conducting a training needs analysis is usually done to gauge what training is needed for employees or to identify and find solutions to:

- Problems with performance
- New system, task or technology
- An organizational need to benefit from an opportunity

NRREP Compliance unit undertakes capacity development focusing on organizations and individuals. Training needs may be assessed by using the following tools:

Observation: First hand observation and analysis in a setting in which the observer is not interfering with normal productivity and used to gather first hand data about an organization's strengths and weaknesses.

Interviews: Using a series of predetermined questions to gauge opinions and perceptions. This tool allows the key stakeholders of an organization to comment on their performance, and allows the interviewer to ask in depth questions about performance.

Questionnaires: Allows for a big picture of the environment by asking respondents identical questions. Allows for more respondents than individual interviews, and takes less time. The data collected can be analyzed in a more quantitative way than with interviews.

Job Descriptions: Study of all responsibilities of a certain job to define employees' expectations and responsibilities, allowing for more thorough training and supervision.

The Difficulty Analysis: identification of an employee's duties that cause them the most difficulty, and allowing for more training in those areas.

Problem Solving Conference: A conference setting that allows employees and other staff to identify a plan for a new task or technology and mould the training to it.

Appraisal Reviews: Within a performance review, questioning the employee about their duties and training. It allows supervisor to uncover reasons for poor performance.

Analysis of Organizational Policy: reviewing the organization's policy on training, and the amount and type of training offered to employees.

When using any of these methods, these three things should be kept in mind:

1. These tools should be used in combination, never rely on just one

2. They may be used to identify training needs in different groups or types of employees

3. They should be applied to individual employees because of variation in training between employees.

Training needs assessment may be carried out using one or more of the above mentioned tools. However, the initial point of going for a training needs assessment would be the findings of the compliance reviews.

7.3. Planning

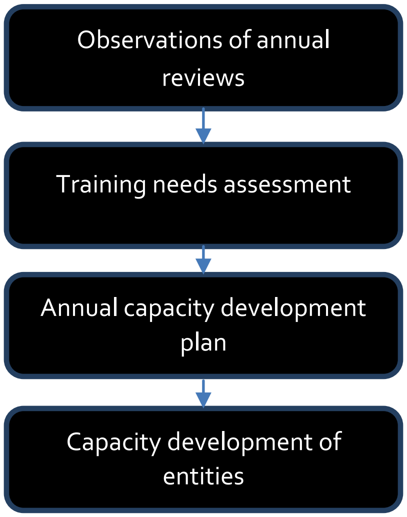
Compliance unit must prepare an annual plan for capacity development activities. Plan for capacity development activities must be prepared keeping in mind the objectives of NRREP programme and training needs assessment. The outcome of capacity development must compliment the objectives of NRREP and should facilitate sustainable development of the renewable energy sector.

The annual plan must be prepared by the Compliance unit in consultation with lead donor and steering committee of NRREP. The annual plan must focus on following aspects:

- Entities to be included in capacity development plan on the basis of needs assessment
- Target group and area for capacity development
- Budget and cost-benefit analysis
- Baseline and target of target areas for capacity development
- Training method

- Selection of trainers for capacity development

Annual plan must be approved by Steering Committee of NRREP. Following steps are taken to finalize the annual capacity development plan.


Observations of annual reviews
Training needs assessment
Annual capacity development plan
Capacity development of entities

7.4. Capacity development program

7.4.1. Capacity development program for audit firms/ organizations on panel of Compliance Unit

Capacity development activities of entities (collectively referred to the audit firms and organisations) shall be carried out as per the annual capacity development plan prepared by Compliance unit and approved by Steering committee. Capacity development of entities would be primarily conducted through workshops. Workshops are to be conducted either at central level in Kathmandu or at regional levels. In order to benefit a larger group, thematic workshops should be conducted for more than one entity at a time.

Workshop purpose and objective

The workshop is designed to engage stakeholders (including empanelled audit firms and auditees) in the identification and sequencing of robust adaptation options for addressing the potential challenges in the NRREP implementation, vulnerabilities therein and skill gaps in effective auditing as may be identified during the quality assurance reviews by the Compliance Unit. More specifically, the workshops shall be designed to achieve the following objectives:

1. To identify and understand development challenges and vulnerabilities in the NRREP programme.

2. To identify corresponding challenges in the existing audit skill sets of the audit firms and its personnel

3. To identify and develop and robust adaptation options that addresses the above challenges, vulnerabilities and skill set development needs.

4. To prioritize and sequence these options into a collection of adaptation pathways which are implementable.

Activities for workshop

Following activities shall be conducted to hold workshop for capacity development of entities:

1. Decide location and timing of workshop as per the annual capacity development plan
2. Decide the scale of workshop: national, sub-national /regional or local
3. Identify appropriate trainers and confirm their availability
4. Contract the trainers to conduct workshop
5. Prepare guidelines for content of each workshop
6. Finalize the workshop content
7. Identify target participants
8. Send invitations
9. RSVP deadline; identify/ invite additional participants if needed
10. Select and book a venue
11. Book audio/ visual equipment commensurate to the scale of workshop
12. Identify need for preparation of training material
13. Prepare, review and finalize the training material to be handed over to participants
14. Arrange logistics for the workshop (pen, paper, slide handouts etc.)
15. Translate content of workshop into vernacular language (if required)
16. Identify team to conduct workshop
17. Mobilize team
18. Conduct dry run of workshop
19. Setup the venue for workshop
20. Conduct workshop
21. Get feedback from participants on pre-printed forms
22. Review participant feedback to ascertain effectiveness of programme
23. Prepare lesson learnt note from participant feedback and use to plan capacity building plan for next year

7.4.2.Capacity development program for individuals

Capacity development activities of individuals shall be carried out as per the annual capacity development plan prepared by Compliance unit and approved by Steering committee. Capacity development of individuals would be primarily conducted through the following steps.

Staff Selection, Training and Professional Development

During the year-end reviews, ISCA and NCA shall assess the number of staff of the Consultants (auditing firms already selected) required to execute the audit plan for the next year and compared with the available competent officers of the audit firms. Resource gaps (temporary and permanent) shall be identified and sources of harnessing the vacancies shall be finalised. The vacancies may be filled by strategically augmenting the outsourcing work to competent government or private agencies.

There should be a programme to induct adequately qualified officers in the panel of agencies selected for auditing and these personnel should be of adequate qualifications, competencies and experience. These personnel should have got adequate skill training before being given any functional responsibility.

The newly qualified personnel planned to be deployed should undergo induction training for first 3 months. During this period they should be provided modular training on functioning of Government at national & sub-national levels and other auditable entities, Government and private sector Accounts and Audit, Risk Based Internal Audit, existing Internal Audit methodology, Information Technology Audit, Performance Audit, Procurement audit and other functional areas (if needed) etc. The training period should include on-job training to be provided by teaming the fresh recruits with experienced auditors.

Training calendar for personnel shall be developed at the beginning of the year depending on existing knowledge and skill-set. Every year, minimum 40 hours of training conducted by Compliance Unit should be attended by each resource of the audit firms on the panel of Compliance Unit. The audit staff shall also be encouraged to attend a stipulated number of continued professional education programmes of the respective professional bodies of which the audit staffs may be member of. Adherence of the same should be linked to the performance evaluation of the resource and entity at the end of the year and should be monitored.

All auditors should be encouraged to take membership of appropriate professional organisation to keep them updated about the development in audit field.

Skill Assessment and Performance Analysis

Internal audit teams should possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit teams of the empanelled audit firms of Compliance Unit collectively should possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities. Without conducting some type of skills assessment, it would be difficult to demonstrate that the auditor possesses the requisite knowledge, skills, and other competencies.

Performance evaluations are required for every audit staff member of the audit firms to document his or her performance, achievement of agreed upon goals and compliance with professional competency standards acceptable to the Compliance Unit. The Compliance Unit shall frame a framework for this and make the audit firms aware of the same. Performance evaluations of its staff by the audit firms and sharing the same with the Compliance Unit for review and further action as necessary shall serve several major functions:

Employee development - Through performance ratings and constructive comments, the evaluation assists employees in recognizing how their performance levels compare to the expectations of Department/ Office and provides recommendations for further training or actions for improvement.

Performance measurement decisions - The evaluation process uses consistent criteria to measure staff performance and, therefore, provides a basis for making relative rankings among staff members. Relative rankings and individual experience levels shall provide input for direct and indirect benefits to the audit staff including salary and advancement decisions, sponsoring to obtain advanced qualifications etcetera.

Professional standards - The evaluation is one of the components of the overall process of supervision, quality assurance, and development of the audit staff and demonstrates compliance with international standards including that of IIA, INTOSAI, IFAC, OAG Nepal, Auditing Standards Board of Nepal etc

Performance evaluations should be conducted for every audit staff member annually. In addition to the annual performance evaluation, staff members should receive feedback on an interim basis. Following interim evaluation procedures should be implemented by the Compliance Unit and Audit Firms Internal Audit Department.

Periodic evaluations - Every staff member will receive a written performance evaluation from the superior and NCA after completion of the assignment. Cumulative comments from these evaluations provide a basis for the annual evaluation by the audit firm and ISCA.

Continuous Feedback – Regular project update meetings may incorporate an element of evaluation in the form of performance feedback and guidance to create a continuous dialogue on the staff member’s strengths and weaknesses as observed on the job. These timely assessments materially affect the quality of the work done and the improvement of staff performance.

Ongoing discussions of the staff member’s strengths and weaknesses should be documented and used as support for or updates to annual evaluations.

Employee Recognition Programme

Motivating employees through recognition is one of the most effective and cost-efficient means to reinforce an organisation's culture. It rewards the individual behaviours that collectively help an organisation attain its' overall objectives and retain top performers. Audit firms, with support from Compliance Unit may introduce appropriate incentive scheme to recognize the good performance of the audit staff. These may include:

Star Performer Award to the audit staff who complies with the professional standards and comply with the audit plan. This award may be given on quarterly basis.

Best Auditor Award to the audit staff who enhances his audit skills by complying with the training programmes, consistently demonstrates integrity, objectivity and independence in audits executed by him. This award may be given on half yearly basis.

Auditor of the year Award to the individual adheres 100% to the quality assurance standards of the Compliance Unit, complies with the training programmes and consistently demonstrates the values of Compliance Unit and the audit firm he belongs to.

8. Annexes

Annex 1: Illustrative NRREP – Audit Plan

Illustrative NRREP – Audit Calendar Financial Year – 2xxx - xx				
Quarter 1				
S. No.	**Component***	**Risk Assessment**	**Implementing Agency***	**Audit type***
1.	Biomass			Financial
2.	Solar			Procurement
3.	PEU			Financial
Quarter 2				
4.	Solar			Financial
5.	Carbon and climate change			Financial
Quarter 3				
6.	Institutional support			Performance
7.	CREF			Regulatory
8.	Community electrification			Financial
Quarter 4				
9.	Gender and social inclusion			Procurement
10.	CREF			Financial

* To be prioritized as per risk assessment and judgment of conducting the audit type on audit entity

Annex II: Risk and Control Matrix (illustrative)

No.	Primary Objective	Main Classification	Control gap	Control gap Classification	Control Reference	Control description	Nature of Control			Frequency	Control Performed by	Control Evidence	Control Evidence Reference	Effectiveness Rating	Rating Justification	Mitigation plan
							IT / Manual / IT Enabled	Prevent / Detect	*Key (Y/N)*							
A	Parameter															
A 1	Sub parameters															
						Control A										
						Control B										