Date: 7th April, 2014

Last date for submission of views/ comments/ suggestions extended upto 16th April 2014

On

EXPOSURE DRAFT
Guidance Note on Internal Audit of Telecommunication Industry

Please submit your views/ comments/ suggestions preferably by email at pd.budhiraja@icmai.in or pd@icmai.in latest by ***April 16, 2014.***

Views/comments/suggestions should be addressed to:

CMA J.K. Budhiraja
Director (Professional Development) and
Secretary to Professional Development Committee
The Institute of Cost Accountants of India,
CMA Bhawan, 3rd Floor,
3, Lodhi Road, Institutional Area,
New Delhi- 110003
Email: pd.budhiraja@icmai.in

Date: 18th March, 2014

EXPOSURE DRAFT
Guidance Note on Internal Audit of Telecommunication Industry

The following is the Exposure Draft of Guidance Note on Internal Audit of Telecommunication Industry issued by the "Professional Development Committee" of the Institute of Cost Accountants of India, for comments and suggestions. The comments/ suggestions on any aspect of this Exposure Draft would be most helpful if they indicate the specific paragraph or group of paragraphs including page number to which they relate, also contain a clear rationale and, where applicable, provide a suggestion for alternative wording.

The proposed Guidance Note may be modified in light of comments/ suggestions received before the same being issued as Guidance Note on Internal Audit of Telecommunication Industry.

Please submit your views/ comments/ suggestions preferably by email at pd.budhiraja@icmai.in or pd@icmai.in latest by ***April 7, 2014.***

Comments should be addressed to:

CMA J.K. Budhiraja
Director (Professional Development) and
Secretary to Professional Development Committee
The Institute of Cost Accountants of India,
CMA Bhawan, 3rd Floor,
3, Lodhi Road, Institutional Area,
New Delhi- 110003
Email: pd.budhiraja@icmai.in

EXPOSURE DRAFT

GUIDANCE NOTE

ON

INTERNAL AUDIT OF

Telecommunication Industry

LAST DATE FOR COMMENTS: APRIL 07, 2014

PROFESSIONAL DEVELOPMENT COMMITTEE

The Institute of Cost Accountants of India

(Statutory body under an Act of Parliament)

HQ: CMA Bhawan, 12, Sudder Street, Kolkata-700 016

Delhi Office: CMA Bhawan, 3, Institutional Area, Lodhi Road, New Delhi-110003

Index of Chapters

Chapter 1
Introduction to Internal audit

1.1 Definition of Internal audit

The need for internal audit is to provide independent assurance that the organization's risk management, governance and internal control processes are operating effectively and efficiently.

Internal audit is a significant tool in evaluating the adequacy of system controls and points out the state of compliance with the applicable laws and regulations, policies and procedures and ensures risk management and promote efficiency.

As defined by the Institute of Internal Auditors (IIA), "*Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes*".

1.2 Need and Objectives of Internal audit

Internal auditing encompasses to:

i. Monitor, assessing, and analyzing organizational risk and controls; and
ii. Review and confirming information and compliance with policies, procedures, and laws.
iii. Assure to the Board, the Audit Committee, and Executive Management that risks are mitigated and that the organization's corporate governance is strong and effective. Assurance of compliance with policies, plans, laws, and regulations;
iv. Safeguard the assets of the business entity;
v. report instances of suspected or proven financial irregularities
vi. Recommend economical and efficient use of entity resources by pursuing established corporate processes, policies, and procedures
vii. Make recommendations for enhancing processes, policies, and procedures where there is room for improvement.

1.3 Five key actions for an internal audit

While executing an internal audit it is necessary for the person Incharge of internal audit to carry out the following five actions before start of an internal audit:

a) **Audit schedule:** The purpose of the audit schedule is to chalk out a timetable after discussions with the auditee before taking up an internal audit and identify the functions/ areas in the organization to be audited. The audit Incharge will guide the effort and ensure the processes which would be included in the audit. The audit schedule gives an insight about type of

resources needed for the audit. A well defined audit schedule is helpful in yielding the desired results within the scheduled time frame.

b) **Audit plan:** A well defined audit plan would cover audit's scope, objectives and agenda. The plan provides a list of events of the audit from its starting to its completion. It also provides about the specific processes and sub-processes which will be audited, when will be audited and by whom these will be audited and the core areas that will be audited in each segment / function.

c) **Audit management:** The audit in-charge shall manage the overall audit process including supervising and communicating any changes/ modifications in the audit plan, sharing the audit progress with the Board, the Audit Committee, and Executive Management or to such other person who is authorized. The audit in-charge shall also, ensure that these are carried our as per the audit schedule and stays on track. In case of any non-conformity the audit in-charge shall ensure that these are logical, valid and clear. Any sort of conflicts shall be addressed and solved constructively by ensuring that the entire audit is conducted professionally and ethically.

d) **Audit Verification:** The department or function / activity being audited is usually supposed to respond to audit nonconformities by mutually agreed date. The response should include identification of the root cause, planned corrective action and a date when the nonconformities shall be removed. The audit in-charge reviews the responses to determine the planned corrective actions are adequate. When the state of affairs are handled by the auditee to eliminate the root cause or fails to identify root cause or proposes a corrective action related to it, the audit in-charge can reject the response and communicate to the manager-of-the-process the reasons as to why the action taken on the matter is inadequate. The second stage of verification occurs when the manager-of-the-process informs the audit in-charge that corrective action has been taken. Based on the action taken report of auditee the audit in-charge or his team member shall verify that the corrective action has been taken and the root cause of the original nonconformity has been removed.

e) **Audit reporting:** The Board, the Audit Committee, and Executive Management or to such other person who is authorized is presented with the written audit observations/ suggestions and informed the issues which needs certain action on the part of the Board, the Audit Committee, and Executive Management etc. on certain non-conformities which guides the basis for discussion of the audit results and when remains unattended forms part of the audit report.

Thus Internal Audit is helpful in providing an independent assessment and view of state of the business, monitoring risks and ensures compliance across organizational and with the use of system software make the internal audit more effective and successful. However an effective common framework is required to carry out the Internal Audit for all types of audits - financial, risk, operations, internal, suppliers, and compliance and the auditing priorities as are determined by a enterprise-level risk-management.

1.4: Principles of Internal Audit

COSO PRINCIPLES OF INTERNAL CONTROL "Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives."

"While internal control is a process, its effectiveness is a state or condition of the process at one or more points in time.''

Internal control systems operate at different levels of effectiveness. Internal control can be judged effective in each of the three categories, respectively, if the board of directors and management have reasonable assurance that:

− They understand the extent to which the entity's operations objectives are being achieved.
− Published financial statements are being prepared reliably.
− Applicable laws and regulations are being complied with.

"While internal control is a process, its effectiveness is a state or condition of the process at one or more points in time." "An internal control system, no matter how well conceived and operated, can provide only reasonable — not absolute— assurance to management and the board regarding achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that judgments in decision-making can be faulty, and that breakdowns can occur because of simple error or mistake.

COSO's internal control framework describes internal controls as consisting of five inter-related components. These are generally called "layers," and the controls within each must be included in management's assessment. The five layers are described by COSO as:

a. Control Environment: "The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors."

b. Risk Assessment: "Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic,

industry, regulatory, and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change."

c. Control Activities: "Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties."

d. Information and Communication: "Pertinent information must be identified, captured, and communicated in a form and time frame that enable people to carry out their responsibilities. Information systems produce reports containing operational, financial, and compliance-related information that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities, and conditions necessary to informed business decision-making and external reporting.

Effective communication also must occur in a broader sense, flowing down, across, and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream.

There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and they must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and shareholders."

e. Monitoring: "Internal control systems need to be monitored — a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures.
Internal control deficiencies should be reported upstream, with serious matters reported to top.

1.5: Internal Audit Strategy and Approaches

There are several different approaches to Internal Audit. International best practice suggests that systems audit is the most effective way that Internal Audit can add value to an organisation. However, it is considered necessary for Internal Audit to complement systems audit with a pre-audit approach. If a pre-audit approach is adopted the Head of Internal Audit, the Audit Committee and the CFO/CEO should discuss the extent that this is necessary. They should also consider suitable means of reducing the proportion of time that Internal Auditors spend on pre-audit work.

The systems approach to Internal Audit seeks to assess and improve the effectiveness of the organisation's internal control system.

The prime purpose of a systems Audit should be to evaluate the extent to which the system may be relied upon to ensure that the objectives of the system are met.

Where internal controls are not adequate and reliable Internal Audit should make practical recommendations to ensure that these controls are improved.

Internal Audit evidence should be adequate to meet the objectives of Audit assignments.

Internal Auditors should be satisfied with the nature, adequacy and relevance of Audit evidence before placing reliance on that evidence. Information should be collected analysed and documented by the use of appropriate Audit techniques.

The production of Audit evidence should be supervised and reviewed by the Head of Internal Audit. To meet an acceptable standard the evidence should be sufficiently adequate and convincing to the extent that a prudent, informed person would be able to appreciate how the Auditor's conclusions were reached.

Internal Audit may also complement its systems approach with other techniques, for example:

- Performance auditing
- Control self-assessment
- Advice and assistance on control issues
- Helping with risk management.

Conclusions are the Internal Auditor's evaluations of the effects of the findings on the particular system reviewed. They should:

- Put the findings in perspective based on the overall implications and significance of the weaknesses identified

– Identify the extent to which the system's control objectives are being achieved and the degree to which the internal control systems should ensure that the goals and objectives of the organisation are accomplished efficiently.

Management should be required to respond in writing to each Internal Audit report.

Management and Internal Audit should agree officer responsibility and target dates for implementation of agreed recommendations. The responsibility for final editing of Audit reports should remain with the Head of Internal Audit who should always retain the right to issue reports without further editing.

Follow-up activity is the process by which Internal Audit confirms that agreed recommendations have been implemented by line managers. Internal Audit should periodically follow up Audit reports to review and test the implementation of agreed Internal Audit recommendations.

The Head of the Internal Audit should submit to the CFO/CEO and Audit Committee, at agreed intervals, a report of Internal Audit activity and results. The report should compare actual Internal Audit activity against the annual Internal Audit plan and should clearly indicate the extent to which the total Internal Audit needs of the public sector organisation have been met.

In the annual Internal Audit report the Head of the Internal Audit should give a formal opinion to the CFO/CEO and Audit Committee on the extent to which reliance can be placed on the organisation's internal control system. The attention of the CFO/CEO and Audit Committee should be drawn to any major Internal Audit findings where action appears to be necessary but has not been undertaken.

1.6 Terms of Engagement of Internal Audit

Before commencement of internal audit, the internal auditor and the Board of Directors or a relevant Committee (auditee) should agree on the terms of engagement. Terms of engagement should be approved by the Board of Directors or a relevant Committee or such other person(s) as may be authorized by the Board in this behalf. The Terms of engagement should contain a statement in respect of the scope of internal audit engagement. The terms of engagement should clearly indicate the responsibility and area of coverage of the entity as well as the internal auditor.

The terms of engagement provide the internal auditor with requisite authority, including unrestricted access to all departments, records, property and personnel and authority to call for information from concerned personnel in the organization.

The Terms of engagement should clearly mention that internal auditor would not be involved in the preparation of the entity's financial statements. It should also be made clear to the Board of Directors or

a relevant Committee or such other person(s) as may be authorized by the Board that the internal audit would not result in the expression of an opinion or any other form of assurance on the entity's financial statements or any part thereof

The internal auditor should have full authority on his processes/ hardware/ systems and audit tools he may use in course of performing internal audit. It should be clear that the ownership of working papers rests with internal auditor and not the entity, however its use shall be limited to the internal audit of the entity or matter relating to it or there is a statutory or a regulatory requirement to do so. It should contain a statement that the internal audit engagement would be carried out in accordance with high professional Standards and ethics applicable to such audit.

The engagement letter of the internal auditor should contain a condition that the report of internal auditor should not be distributed or circulated by the entity or the internal auditor to any party other than that mutually agreed between the internal auditor and entity unless there is a statutory or a regulatory requirement to do so.

The engagement letter of the internal auditor should indicate that the internal auditor would be compensated, including any out of pocket expense, travelling expenses, taxes etc., for the services performed by the internal auditor including the audit team members.

1.7 Independence of Internal Auditor

An independent internal audit function is widely recognized as an integral part of an entity's strategic objectives, corporate governance, and risk management of its business activities.

Internal auditor's role is to evaluate the adequacy and effectiveness of systems and processes of an entity and to identify and manage risks present in conducting business activities.

Professional internal auditors are required to be independent of the business activities of the entity to which they audit. The internal auditor should also be impartial and free of any interest which is incompatible to integrity and objectivity and inform the entity (auditee) of any personal or external factors that impede or likely to impede the independence and objectivity if required remedial action can be taken.

Generally the internal auditors are part of company management and paid by the company. The internal audit activity of the entity is basically reviewing the matters which are critical to the entity due to the oversight of management's activities. The internal auditors should also take reasonable professional care in specifying evidence required, in gathering and evaluating that evidence and in reporting the findings. They need to remain alert to the instances that could indicate errors, fraud, etc. To provide

independence, most Internal auditors report to the Chairman of Board or the chairman of the Audit Committee and can be some other person authorized by the management of the entity.

While evaluating the adequacy and effectiveness of systems and processes of an entity, the internal auditor should act independent of the business activities and be honest and sincere to the assignment, unbiased and should not compromise his integrity, objectivity and hold a neutral position within an organization while discharging his duties as an internal auditor of the entity.

1.8 Legal Requirement for Internal Audit

The compliance with the laws of the home country as well as the laws of the foreign country land for existence of businesses in India and abroad is a critical factor. As per the legal obligation / requirement under different statutes in India and abroad a Company shall have internal audit of its accounts carried out, at such interval and in such manner as may be specified .

Clause 49 of Listing Agreement: Corporate Governance (SCRA)

In case of the listed companies as per the Clause 49 of Listing Agreement the audit committee should be reviewing the adequacy of internal audit function, if any, including the structure of the internal audit department, staffing and seniority of the official heading the department, reporting structure, coverage and frequency of internal audit.

Under Section 177 of the Companies Act 2013 the internal auditor, if any, shall attend and participate at meetings of the Audit Committee of the company.

The provisions for constitution of the Audit Committee under Section 292A of the Companies Act 1956 has been replaced by Section 177 of the Companies Act 2013, which are as follows:

177. (*1*) The Board of Directors of every listed company and such other class or classes of companies, as may be prescribed, shall constitute an Audit Committee.

(*2*) The Audit Committee shall consist of a minimum of three directors with independent directors forming a majority:

Provided that majority of members of Audit Committee including its Chairperson shall be persons with ability to read and understand, the financial statement.

(*3*) Every Audit Committee of a company existing immediately before the commencement of this Act shall, within one year of such commencement, be reconstituted in accordance with sub-section (*2*).

(*4*) Every Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall, *inter alia,* include,—

(*i*) the recommendation for appointment, remuneration and terms of appointment of auditors of the company;

(*ii*) review and monitor the auditor's independence and performance, and effectiveness of audit process;

(*iii*) examination of the financial statement and the auditors' report thereon;

(*iv*) approval or any subsequent modification of transactions of the company with related parties;

(*v*) scrutiny of inter-corporate loans and investments;

(*vi*) valuation of undertakings or assets of the company, wherever it is necessary;

(*vii*) evaluation of internal financial controls and risk management systems;

(*viii*) monitoring the end use of funds raised through public offers and related matters.

(*5*) The Audit Committee may call for the comments of the auditors about internal control systems, the scope of audit, including the observations of the auditors and review of financial statement before their submission to the Board and may also discuss any related issues with the internal and statutory auditors and the management of the company.

(*6*) The Audit Committee shall have authority to investigate into any matter in relation to the items specified in sub-section (*4*) or referred to it by the Board and for this purpose shall have power to obtain professional advice from external sources and have full access to information contained in the records of the company.

(*7*) The auditors of a company and the key managerial personnel shall have a right to be heard in the meetings of the Audit Committee when it considers the auditor's report but shall not have the right to vote.

(*8*) The Board's report under sub-section (*3*) of section 134 shall disclose the composition of an Audit Committee and where the Board had not accepted any recommendation of the Audit Committee, the same shall be disclosed in such report alongwith the reasons therefor.

(*9*) Every listed company or such class or classes of companies, as may be prescribed, shall establish a vigil mechanism for directors and employees to report genuine concerns in such manner as may be prescribed.

(*10*) The vigil mechanism under sub-section (*9*) shall provide for adequate safeguards against victimisation of persons who use such mechanism and make provision for direct access to the chairperson of the Audit Committee in appropriate or exceptional cases:

Provided that the details of establishment of such mechanism shall be disclosed by the company on its website, if any, and in the Board's report.

Section 138(1) of the Companies Act provides that such class or classes of companies as may be prescribed shall be required to appoint an internal auditor, who shall either be a chartered accountant or a cost accountant, or such other professional as may be decided by the Board to conduct internal audit of the functions and activities of the company.

Under SEBI Circular No. MRD/DMS/Cir-29/2008, October 21, 2008 in partial modification of SEBI circular No. MIRSD/ DPSIII/ Cir-26/ 08 dated August 22, 2008 on the above subject, the SEBI has mandated that stock brokers/trading members/clearing members shall carry out complete internal audit on a half yearly basis by chartered accountants, company secretaries or cost and management accountants who are in practice and who do not have any conflict of interest.

Under Circular of SEBI No. SEBI/MIRSD/CRA/Cir-01/2010 dated January 06, 2010 Internal Audit for Credit Rating Agencies (CRAs) has been prescribed under Regulation 22 of the SEBI (Credit Rating Regulations), 1999, which shall be undertaken on a half yearly basis and shall be conducted by Chartered Accountants, Company Secretaries or Cost and Management Accountants who are in practice and who do not have any conflict of interest with the CRA.

Under IRDA (Investment) (Fourth Amendment) Regulations, 2008

a. An Insurer having Assets under Management (AUM) not more than Rs.1000 crore shall conduct a Quarterly Internal Audit to cover both Transactions and related Systems.
b. The Audit Report of the company shall clearly state the observation at transaction level and its impact, if any at System level. The Audit Report shall be based on Exception Reporting.

Corporate Responsibility for Financial Reports (Under Section 302 of Sarbanes Oxley Act of 2002).

(a) Regulations Required.—The Commission shall, by rule, require, for each company filing periodic reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 [15 U.S.C. 78m, 78o(d)], that the principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that—

(1) the signing officer has reviewed the report;

(2) based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;

(3) based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report;

(4) the signing officers—

(A) are responsible for establishing and maintaining internal controls;

(B) have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;

(C) have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and

(D) have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date;

(5) the signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function)—

(A) all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls; and

(B) any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls; and

(6) the signing officers have indicated in the report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

(b) Foreign re-incorporations have no effect.—Nothing in this section 302 shall be interpreted or applied in any way to allow any issuer to lessen the legal force of the statement required under this section 302, by an issuer having reincorporated or having engaged in any other transaction that resulted in the transfer of the corporate domicile or offices of the issuer from inside the United States to outside of the United States.

(c) Deadline—The rules required by subsection (a) shall be effective not later than 30 days after the date of enactment of this Act.

Management Assessment of Internal Controls (Under Section 404 of Sarbanes Oxley Act of 2002).

(a) Rules Required.—The Commission shall prescribe rules requiring each annual report required by

section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) Internal Control Evaluation and Reporting.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board.

Any such attestation shall not be the subject of a separate engagement.

****

Chapter 2
Documentation and working papers

Internal audit documentation covers the internal audit charter, the internal audit plan, the type and extent of audit procedures performed, timings and the conclusions drawn from the evidence obtained. Proper documents act as basis for the planning and performing the internal audit. Documents provide the evidence of the work of the internal auditor. Internal audit documentation should be detailed and comprehensive to obtain an overall understanding of the audit.

The internal auditor should document the issues that are important in providing evidence and support his findings or in preparation of the report. In addition, the working papers also help in planning and carrying out the internal audit, review and control the work and most importantly, provide evidence of the work performed to support his observations/ findings in the report.

Need for Internal audit documentation:

I. Aid in planning and executing the internal audit.
II. Aid in review of the internal audit work.
III. As evidence of work performed during the internal audit to support the internal auditor's opinion and findings.
IV. Assistance to third party while reviewing the internal auditor's work.
V. Can be used as evidence to verity that the internal audit was performed in accordance with the scope of work as mentioned in the engagement letter.

The internal audit documentation should cover all the important aspects of an engagement viz., engagement acceptance, 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. In case the internal audit is outsourced, the documentation should include a copy of the internal audit engagement letter, containing the terms and conditions of the appointment.
Internal audit documentation should be designed in accordance with requirement of specific audit and properly maintained to meet the requirements and circumstances of each audit. All significant issues which require special attention, together with internal auditor's observation thereon should be appropriately included in the internal audit documentation.

Properly designed and maintained internal audit Documentation enables the reviewer to understand:

a) the nature and extent of audit procedures performed and applicable legal and regulatory requirements;
b) timings of the audit

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

d) important issues arising during the course of audit and conclusions drawn; and

e) terms and conditions of an internal audit engagement, scope of work, reporting requirements and any other special conditions relating to conduct of the internal audit.

f) Record of the work performed.

Use of Working Papers as evidence

The internal audit Documents provide the evidence of the work of the internal auditor and are important in providing evidence to his opinion or the findings. Following are the advantages of having sufficient and properly maintained working papers:

i. Assistance in the performance of the audit.

ii. Forming basis of the auditor's observations/ findings in his report.

iii. Providing information for the report.

iv. Aiding the review and evaluation of the work done.

v. Aiding cross referencing between audit evidence and decision taken by the internal auditor.

vi. Providing record of work done

The internal auditor should formulate policies as to the custody and retention of the internal audit documentation within the framework of the overall policy of the entity in relation to the retention of documents and in accordance with the practices prevailing in the profession.

Note: For more details, the readers may refer to Cost Audit and Assurance Standard (CAAS 102) on "Cost Audit Documentation" issued by the Institute of Cost Accountants of India

****

Chapter 3
Planning an Internal Audit and Audit Programme

While carrying out the internal audit of an entity, an internal audit plan is required to be formulated. Internal audit plan is a document which defines the scope, coverage and resources, duration of audit, required for an internal audit of an organization over a defined time period. The internal auditor should formulate the plan in consultation with those charged with governance e.g. board, audit committee or any other person authorized by the management and develop document for each internal audit engagement to help him conduct the engagement in an efficient and time bound manner. The formulation of internal audit plan ensures that proper attention is given to significant areas of internal audit and identification of potential problems and use of techniques and available skills judiciously so that the audit assignment can be completed with the stipulated time and as per the terms of engagement**.**

The internal audit plan should be comprehensive and clearly defined so that the objectives of the internal audit can be achieved efficiently and effectively. The internal audit plan should be consistent with the desired goals and objectives of the internal audit function as well as the goals and objectives of the entity. It should be ensured that the plan is consistent with the terms of the engagement and should also reflect the risk management strategy of the entity.

The internal audit Planning involves developing a plan for taking action to cover the expected scope and conduct of audit and developing an audit program consisting the nature, extent of audit procedures and timing. Planning is a continuous exercise. An audit plan should be continuously reviewed by the internal auditor to make out any modifications required to bring the same in line with the changes, if any, in the scope of audit or change in the audit environment of the entity. However, any major modification to the internal audit plan should be done only after consideration and in consultation with the board, audit committee or any other person authorized by the management if so required. Any modification in the internal audit plan should be documented by the internal auditor, if such modifications are significant.

The internal audit plan should be drawn keeping in view the size and nature of the business of the entity. While developing the internal audit plan, the internal auditor should have regard to the objectives of the internal audit engagement as well as the resources and time, keeping in view the size of the entity.

While drafting an internal audit plan following aspects should be covered:

i. Provide information about the legal and regulatory framework within which the entity operates.
ii. Provide information about of the entity's accounting and internal control systems and policies.
iii. Assessment of the effectiveness of the internal control procedures in practice in the entity.
iv. Documentation of the nature, extent of procedures to be performed and timeline for completion of assignment.

v. Assessment about the activities requiring special focus on the criticality of such activities as well as on their materiality and their effect on operations of the organization.

vi. Identifying staff which is most suitable for the assignment undertaken.

vii. Provide information about the identification of persons assigned with reporting responsibilities.

The internal audit plan should also envisage about the benchmarks against which the actual results of the activities can be measured, the time spent, the actual cost incurred on completion of the assignment.

The internal auditor should prepare a formal internal audit program listing the procedures essential for achieving the objective of the internal audit plan and ensure that the internal audit is carried out in accordance with the standards of Internal Audit. The form and content of the audit plan and the extent of its details would depend on the nature, business environment and size of organization however, the internal audit program should be so designed that it facilitates in achieving the desired objectives of the engagement.

Note: For more details, the readers may refer to Cost Audit and Assurance Standard (CAAS 101) on "Planning an Audit of Cost Statements"

****

Chapter 4
Audit Sampling

In the modern business environment, the internal auditing is going to be tough as huge and large number of transactions are carried out by the business entities which makes the task of internal audit very difficult and time consuming so the internal auditors have to be cautious and careful because there is a time limit for completing the audit assignments as well as they have to take care about quality also and prove their professional efficiency to effectively handle the internal audit assignment of big business entity.

In modern age, the auditor seldom performs audit checks on all items of an account or transactions for the purpose of assessment of the population (an account balance or transactions). Consequently, the evidential matter obtained for an account balance or transactions is based upon the reasoning that the characteristics found in a representative sample of a population (an account balance or transactions) are reasonably true representation of characteristics to be found in the population from which such sample is taken.

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

When designing an audit sample, the internal auditor should consider the following:

(i) the specific audit objectives,
(ii) the population from which the internal auditor takes sample,
(iii) the sample size and,
(iv) use of sampling technique (statistical vs. non statistical sampling).

Therefore while deciding about picking an audit sample the internal auditor has to ensure that testing the sample will provide appropriate audit evidence. Therefore when determining the sample size, the internal auditor should consider sampling risk, the tolerable error, and the expected error.

The internal auditor should select sample items in such a way that the sample can be expected to be representative of the population. This requires that all items or sampling units in the population have an opportunity of being selected.

The internal auditor should evaluate the sample results to determine whether the assessment of the relevant characteristics of the population is confirmed or whether it needs to be revised.

Despite sampling being unavoidable in most of the audits, it is one area which is a challenge for the auditors and many auditors struggle with as choosing the most appropriate sampling method, picking the appropriate and adequate audit sample, testing the sample and then evaluating the results of the audit sample to ensure that it yields the desired results.

****

Chapter 5
Audit Evidence

While compiling suitable and adequate evidence the internal auditor should assess whether he has obtained adequate and appropriate audit evidence to draw his conclusions or form an opinion or have a basis of his findings in accordance with the scope of the terms of the engagement.

The internal auditor should assess that internal audit evidence obtained from one source is inconsistent with that obtained from another, or the internal auditor has doubts over the reliability of information to be used as internal audit evidence when the internal audit is carried out of an entity / department/ function/ activity the internal auditor draws conclusions or form an opinion with regard to the key issues and areas of concern, significant control lapses, weaknesses / failures in the system or procedures, the internal auditor shall make modifications in the existing in the system or procedures or apply additional audit procedures which in his opinion are necessary to resolve the issue.

The internal auditor can obtain evidence by performing the following procedures:

a. Inspection and verification of information / data / record
b. Observation
c. Inquiry and confirmation
d. Assessment, findings and computation
e. Analysis and conclusion

During the course of internal audit the internal auditor should have / collect all the evidence that he considers necessary for the expression of his opinion. Professional skill and judgment is also required to determine the nature and amount of audit evidence required to draw his conclusions or form an opinion or have a basis of his findings. In this regard, the internal auditor should consider:

i. The issue under consideration;
ii. Materiality / impact of possible lapses/ errors / frauds;
iii. Degree of risk of lapses/ errors / frauds;
iv. Probability of the error occurring;
v. Reliability; and
vi. Appropriateness and support to draw conclusion or to form an opinion or have a basis of findings

Use of Working Papers as Evidence

The internal auditor should document the working papers that he considers important in providing evidence to his opinion or the findings. Advantages of having sufficient and properly maintained working

papers include the following:

a. Aid in the performance of the audit.
b. Record of work done.
c. Basis of the internal auditor's observations/ findings in his report.
d. Input for the report.
e. Aid in cross referencing between audit evidence and opinion taken by the internal auditor.
f. Aid in the assessment and evaluation of the work done

Thus while preparing the report the internal auditor should have satisfactory and suitable working papers as evidence to enable him to draw reasonable conclusions out of the documentary evidences and his findings.

****

Chapter 6
Analytical Procedures

For execution of internal audit processes certain analytical techniques need to be developed. Analytical procedures means the analysis of significant ratios and trends, including the resulting investigation of fluctuations and relationships in both financial and non-financial data that are inconsistent with other relevant information or which deviate significantly from predicted amounts. Analytical procedures help in an efficient and effective assessment of information collected during the course of internal audit. The internal auditor should ascertain that analytical procedures developed by the internal auditor and applied during the course of internal audit of an entity are effective and yielding the expected results. The application of analytical procedures is an instrument for risk assessment procedures at the planning and overall review stages of the internal audit.

The application of analytical procedures in the internal audit help the internal auditor to arrive at the conclusion as to whether the systems, processes and controls are robust, operating effectively and are consistent with the expectation of internal auditor about the result of the business.

The analytical procedures are useful tool to identify significant fluctuations or the irregularities or the inconsistencies with other relevant information or that deviate from predicted amounts, the internal auditor should investigate and obtain adequate explanations and appropriate corroborative evidence. The examination and evaluation should include inquiries of management and the application of other auditing procedures until the internal auditor is satisfied that the results or relationships are sufficiently explained. Unexplained results or relationships may be indicative of a significant condition such as a potential error, irregularity, or illegal act. Results or relationships that are not sufficiently explained should be communicated to the appropriate levels of management. The internal auditor may recommend appropriate courses of action, depending on the circumstances.

****

Chapter 7

Accounting System and Internal Control

Introduction

While the management is responsible for establishment and maintenance of appropriate internal control and risk management systems, the role of the internal auditor is to suggest improvements to those systems. For this purpose, the internal auditor should:

(i) Obtain an understanding of the risk management and internal control framework established and implemented by the management.

(ii) Perform steps for assessing the adequacy of the framework developed in relation to the organizational set up and structure.

(iii) Review the adequacy of the framework.

(iv) Perform risk-based audits on the basis of risk assessment process.

Internal auditor may, however, also undertake work involving identification of risks as well as recommend design of controls or gaps in existing controls to address those risks.

Internal Control System

An internal control system is crucial to the successful functioning of any enterprise. It refers to the policies and procedures as well as the attitude of the management to assist in achieving the following overall objectives of the management:

(i) Orderly and efficient conduct of the business

(ii) Adherence to management's policies and directives

(iii) Safeguarding assets

(iv) Prevention and detection of frauds and errors

(v) Accuracy and completeness of the accounting records

(vi) Timely preparation of reliable financial information

(vii) The absence, inadequacy or malfunctioning of the internal control system could, therefore, have adverse results.

(viii) To be able to effectively help the management achieve its above mentioned objectives, it is essential that the internal control system has the following elements:

a) Integration with the risk management policy of the entity.

b) Constant monitoring of various activities and functions.

c) Identification and analysis of variances.

d) Determination and implementation of corrective action.

e) Revision of objectives and norms where needed and where supported.

In addition, the internal controls must also satisfy the three basic criteria:

(i) they must be appropriate, i.e., the right control in the right place and commensurate to the risk involved;
(ii) they must function consistently as planned throughout the period, i.e., be complied with carefully
(iii) by all employees involved and not by-passed when key personnel are away or the workload is heavy; and
(iv) They must be cost effective, i.e., the cost of implementing the control should not exceed the benefits derived.

The internal control system should focus on both accounting and non-accounting operations and functions.

Strong accounting controls result in correct, reliable, timely and relevant reporting of financial transactions that have already occurred while strong controls in operational areas improve the overall performance of the enterprise.

The internal auditor should review whether the internal controls are cost effective. Evaluation of cost effectiveness should take into consideration both direct and indirect costs. Review of internal controls may include interviews with personnel at various organizational levels, transaction walkthroughs, review and analysis of documented policies and procedures and mapping the process to determine and rectify existing control gaps and to suggest process improvement. The internal auditor should determine if the controls were in use throughout the period of intended reliance or have there any substantial alterations in the same during the stated period. Different techniques may be used to record information. Selection of a particular technique depends on the auditor's judgment.

Evaluation of Internal Control

Internal auditors should systematically evaluate the nature of operations and system of internal controls in the departments being audited to determine the nature, extent and timing of audit procedures. Internal controls of an organization comprise the plan of organization and methods adopted to safeguard assets, comply with laws, ensure the completeness and correctness of data, promote efficiency and encourage adherence to management policies. It is important that a review of an internal control system be directed primarily towards those controls that have an important bearing on the reliability of the system (i.e., key controls).

Internal Control Assessments

The internal auditor assess the 'as –is' internal control system within the organization and map it against a globally accepted 'standard' which is basically, an Internal Controls framework- COSO being the most widely used.

Evaluate efficiency and effectiveness of controls

Recommend new controls where needed – or discontinuing unnecessary controls

Use of control frameworks

Control self-assessment (CSA)

The most contentious aspect of SOX is Section 404, which requires management and the external auditor to report on the adequacy of the company's internal control over financial reporting (ICFR). This is the most demanding aspect of the legislation for companies to implement, as documenting and testing important financial manual and automated controls requires enormous effort. Under Section 404 of the Act, management is required to produce an "internal control report" as part of each annual Exchange Act report. The report must affirm "the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting." The report must also "contain an assessment, as of the end of the most recent fiscal year of the company, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting." To do this, managers are generally adopting an internal control framework such as that described in COSO. Both management and the external auditor are responsible for performing their assessment in the context of a top-down risk assessment, which requires management to base both the scope of its assessment and evidence gathered on risk. Both the PCAOB and SEC recently issued guidance on this topic to help alleviate the significant costs of compliance and better focus the assessment on the most critical risk areas.

The recently released Auditing Standard No. 5 of the Public Company Accounting Oversight Board (PCAOB), which superseded Auditing Standard No 2, has the following key requirement for the external auditor:

(i) Assess both the design and operating effectiveness of selected internal controls related to significant accounts and relevant assertions, in the context of material misstatement risks;
(ii) Understand the flow of transactions, including IT aspects, sufficiently to identify points at which a misstatement could arise;
(iii) Evaluate company-level (entity-level) controls, which correspond to the components of the COSO framework;
(iv) Perform a fraud risk assessment;
(v) Evaluate controls designed to prevent or detect fraud, including management override of controls; Evaluate controls over the period-end financial reporting process;
(vi) Scale the assessment based on the size and complexity of the company;
(vii) Rely on management's work based on factors such as competency, objectivity, and risk;
(viii) Evaluate controls over the safeguarding of assets; and

(ix) Conclude on the adequacy of internal control over financial reporting.

Internal Control Certifications

Under Sarbanes-Oxley, two separate certification sections came into effect—one civil and the other criminal. Section 302- (civil provision); Section 906- (criminal provision).Section 302 of the Act mandates a set of internal procedures designed to ensure accurate financial disclosure. The signing officers must certify that they are "responsible for establishing and maintaining internal controls" and "have designed such internal controls to ensure that material information relating to the company and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared." The officers must "have evaluated the effectiveness of the company's internal controls as of a date within 90 days prior to the report" and "have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date."

****

Chapter 8
Internal Control & Risk Assessment

Internal Control

The Internal auditor is required to examine the continued effectiveness of the internal control system through evaluation and make recommendations, if any, for improving that effectiveness. Internal auditors should systematically evaluate the nature of operations and system of internal controls in the entity being audited to determine the nature, extent and timing of audit procedures. Internal controls of an organization comprise process and methods adopted to safeguard assets, comply with laws and encourage adherence to management policies, ensure the completeness and correctness of data and promote efficiency. The internal auditor is required to have focus on improving the internal control structure and promoting better corporate governance in the entity. The internal auditor should cover following aspects while evaluating and making recommendation on the internal control system:

- Evaluation of the efficiency and effectiveness of controls.
- Recommending new controls where needed – or discontinuing unnecessary controls.
- Using control frameworks.
- Developing control self-assessment

The evaluation of internal control in an entity involves:

i. Understanding of the existing design and operation of the internal control system of the entity;
ii. assessing the degree of control effectiveness through testing of controls;
iii. determining the significance and the sensitivity of the risk for which controls are being assessed;
iv. assessing the susceptibility to misuse of resources, identifying the areas which are prone to committing of fraud, failure to attain objectives regarding ethics, economy, efficiency and effectiveness, or failure to fulfill accountability obligations;
v. non-compliance with laws and regulations, laid down policies and procedures;
vi. assessing the adequacy of the control design; and
vii. observations on the internal control evaluation, suggestions and recommendation for necessary corrective actions.

There is always need for an understanding of the significant processes and internal control systems which are sufficient to plan the internal audit engagement and develop an effective audit approach. The internal auditor should use his professional acumen and judgment to assess and evaluate the efficacy of the internal control operating of the entity. The auditor should have information about the control environment which is satisfactory to assess management's attitudes, awareness and actions relating to internal controls and their significance in the entity and should also have an understanding of the internal control procedures adequate to develop the audit plan for the entity.

Following aspects are required to be taken into consideration while evaluating of internal control system in an entity:

a) Information about the entity's mission statement and written goals and objectives.
b) Assessment of risks at the entity level.
c) Assessment of risks at the function or activity level.
d) Prepare a Business Controls worksheet for each significant activity in each function or department of the entity with documentation of the associated controls procedures and their degree of adequacy, give special attention for those activities which are most significant to the success of the activity, function or department.
e) Study of business controls worksheet to assess the risks, for which no controls exist or the existing controls are inadequate.
f) Ensure that predictable risks identified at the function or department or entity level are addressed in the Business Controls worksheet and operating controls documents.

The internal control weaknesses should be identified which have not been corrected and necessary steps required for correcting those weaknesses. The internal auditor should document the rationale in deciding which audit recommendations should be followed up on and when, in contrast with recommendations where no follow-up is needed. In the situation when recommendations have been effectively implemented or that senior management has accepted the risk of not implementing the recommendations, the internal auditor should document the matter and appropriately report its impact on the internal audit process.

Risk assessment:

Risk is an event which can prevent, hinder and fail to further or otherwise obstruct the entity in achieving its objectives. Risk can be classified as Strategic, Operational, Financial and information. Management is responsible for establishing and operating the risk management framework.

Enterprise Risk Management is a process consists of Risk identification, prioritization and reporting, Risk mitigation, Risk monitoring and assurance. The corporate risk function establishes the policies and procedures, and the assurance phase is accomplished by internal audit. The role of internal auditor is to provide assurance to management on the effectiveness of risk management. While assessing the effectiveness of the enterprise risk management following aspects is required to be examined:

(i) assessment of the risk both at the entity level as well as the function level;
(ii) assessment of compliance with the risk management policy and framework; and
(iii) assessment of adequacy of internal audit plan;
(iv) assessment of the efficiency and effectiveness of the risk response; and

Enterprise Risk Management is a planned, consistent and constant process of evaluating or assessing risk and developing strategies to manage risk within manageable limit. It involves identification, assessment, mitigation, planning and implementation of risk and developing an appropriate risk response policy.

The internal auditor should only assess and identify the risks and not manage any of the risks or take risk management decisions on behalf of the management. The accountability for risk management decisions should be of the management and should not be taken by the internal auditor. Internal auditor's role is only to comment and advise on risk management and assist / guide management to mitigate of risks.
The internal auditor should normally perform an annual risk assessment of the entity, to develop a plan of audit engagements for the forthcoming period if the circumstance so require. The plan needs to be reviewed at various frequencies carried out. This involves review of the various risk assessments performed by the entity (e.g., strategic plans, competitive benchmarking, etc.), consideration of prior audits, and interviews with a variety of senior management. It is designed for identifying internal audit key areas and managing risks directly for the enterprise. The risk assessment process should be of a continuous nature so as to identify not only residual or existing risks, but also emerging risks. The risk assessment should be conducted formally at least annually but in complex enterprises it can be conducted more than once depending upon the gravity of situation.

The internal auditor should properly understand and study the Enterprise Risk Management to give assurance to management on the efficacy of risk management in the entity. The internal auditor should keep his independence and objectivity ensuring the management of the entity about the effectiveness of the Enterprise Risk Management. The internal auditor should ascertain that risks are appropriately assessed and managed. The internal auditor as a result of the review, Tests conducted, Samples covered and Observations and recommendations, delineating the following information Assurance rating (segregated into High, Medium or Low) can submit his report to the Board or its relevant Committee or some other authorised person in this behalf by the entity.

****

Chapter 9

Internal Audit in IT Environment and Requirement for Successful System Audit

(A) Internal Audit in IT Environment

In the modern business environment the information technology (IT) is almost used in all spheres of operations of an entity, from data entry, data processing to resource planning to online sales, e-commerce, MIS for management and control of business activities of the entity either through the standard software available in the market or through a tailor made software for the entity.

However excessive reliance on the use of information technology without taking proper safety/protection can land up an entity in loss if data, systems failure or hacking of system/ data and compliance with the cyber laws of the land etc. Entity-level control procedures for information technology are the foundation for internal control, providing discipline and structure to the organization. The information technology controls have a pervasive effect on the reliability, integrity and availability of processing and relevant data. The internal auditor should properly assess the effect of an IT environment on the internal audit engagement. The internal auditor should understand and analyse the use of information technology environment to record, compile, process and analyse information; and assess the effectiveness of the system of internal control in existence in the entity relating to:

(i) Input of authorised, correct and entire data to the processing centre;
(ii) Reliability and authenticity of software (not pirated software) used in processing, analysis and reporting of data;
(iii) Verifiability/ audit trail of computer-based accounting reports.

Business process controls provide structure to generate revenue, costs and other financial records and ultimately report on the financials of the organization. These documented templates or flow charts are helpful to the internal auditor to be acquainted about the existence of information technology system controls their design and the related test procedures and management action plan for thwarting weaknesses and deficiencies.

While evaluating the reliability of the internal control systems in IT environment, the internal auditor should ascertain the following:

(i) ensure that authorised, relevant, accurate and entire data is processed,
(ii) ensure the accuracy and completeness of output,
(iii) provide for timely detection and rectification of errors,
(iv) generate alert signal for unauthorised amendments to the programs/ software,
(v) ensure safe custody of source code of application software and data files,

(vi) provide for proper backup of data/ information in case of interruption in the system due to power, mechanical or processing failures or restart of the system,

(vii) ensure adequate security measures to protect data against fire and other calamities, frauds etc.

The internal auditor should assess the effectiveness and safety of the information technology resources, including – manpower, applications, facilities and data and review that the information technology system in the entity considers the confidentiality, effectiveness, integrity, availability, compliance and validity of data and information processed and handling of processed data/ output.

The internal auditor should have professional knowledge/ expertise of the information technology systems such as the operating knowledge of a specialized ERP / SAP system or other similar accosting system etc. to plan, direct, supervise, control and review the work performed through IT system. When the information technology systems are significant, the internal auditor should also obtain an understanding of the IT environment. In case the internal auditor is not professionally equipped to handle the information technology system of the entity he should seek the assistance of a technical expert possessing professional skills in the field of system audit, who can be either on the roll of the internal auditor or an outside professional.

While designing audit procedures to review the systems, processes, controls and risk management framework of the entity the internal auditor should understand properly the IT environment of the entity with the help of checklist and questionnaire.

In case the internal auditor finds during the course of audit that the information technology systems or information processing of the entity or a particular operation has been outsourced to an outside party, the internal auditor should give due consideration to the risks associated with such outsourced services in light of the review of outsourced IT control processes with regard to the processing of data, security of data and report generated. The internal auditor should ensure as to what extent to the entity's controls provide reasonable assurance with regard to the completeness, validity, reliability and verifiability of the data and information processed by such outsourced agency.

(B) **Requirement for successful System Audit**

A successful internal audit program is that which yields the predetermined and desired results and support continuous updating in the changed scenarios/ conditions by use of software and automate the end to end audit process. The audit program shall be effective only when it yields impressive results of the audit process without much human interference. The common internal audit outcomes are:

a) assessment of effectiveness and adequacy of internal control;

b) risk management and control assurance;

c) legal and regulatory compliance assurance;

d) legislature readiness assessment and ongoing testing, such as Companies Act and SEBI Act and its Directives;
e) development of awareness of risk and control across the entity;
f) ability to respond to urgent matters.

The use of system in the internal audit is most desired in the present scenario. An internal audit shall be more successful and effective if aforementioned five key activities are automated using software to make them effective for different audits. The experts have identified the following core requirements of a software solution for a closed-loop internal audit program for end-to-end process, audit management through corrective actions and change control.

Audit Management: The software should cover definition and management of various elements of the audit process such as creation of different checklists, tracking audit schedule details, managing role differentiation between audit in-charge, approvers and managers for all audit matters and enabling proper distribution of workload by sharing audit matters. The software should support auditors to track progress/ audit schedule details, identify and append various documentary evidence as supporting proof of the non-conformities, review non-conformities highlighted by the internal audit team, ensure all exit criteria in the checklist have been achieved before the step is completed and report audit results.

Identification of Non-conformance and handling: The software should track and identify all non-conformances noticed during the audit process and provide ability to either to report the non-conformance and its gravity or suggest a corrective action process.

Corrective Action: The internal audit software should provide a mechanism for automatically routing a corrective action request to the authorized users with built-in MIS reporting and escalation procedures for unresolved issues, review all relevant non-conformance records to analyze the root cause and document corrective actions to rectify the problem or prevent its recurrence. The system should support configurable industry-specific report formats which are widely used by the consultants.

Change Control: The software should support multiple change control mechanisms required for corrective action such as document change, process instructions change or change to a standard operating procedure etc.

The system should be developed to cover all important aspects of audit using web architecture and it can be easily accessed by any user and the system should be such that it can be easily integrated with other systems or corporate portals.

The system should report on any non-conformance and corrective action at a function /department/ plant/division level and provide display on dashboard of the monitor to report on key process indicators of the internal audit activities.

****

Chapter 10

Relying on External Opinion and Reference in Audit Report

In order to effectively discharge of his duties as internal auditor, the internal auditor has right to obtain technical advice and assistance from competent experts if the internal audit team does not possess the necessary knowledge, skills, expertise or experience needed to perform all or part of the internal audit engagement.

When the internal auditor uses the opinion of an expert, he should satisfy himself about the competence, objectivity and the independence of such expert and consider the impact of such assistance or advice on the overall result of the internal audit engagement, especially in cases where the outside expert is engaged by the senior management of the entity. While determining the use of opinion of an expert or not, the internal auditor should consider:

(i) the materiality of the item being examined by the expert.
(ii) the nature and complexity of the item including the risk of error therein.
(iii) the other internal audit evidence available to support/ oppose the opinion of the expert.

The internal auditor should satisfy himself as to the skills and competence of the expert with regard to:

(i) the professional qualifications or membership of the expert in a professional body.
(ii) the reputation of the expert in the relevant discipline.
(iii) the knowledge and specific experience of the expert in the industry in which the entity operates

The internal auditor should ensure himself that the work of the expert constitutes appropriate evidence in support of the overall conclusions formed during the internal audit engagement with regard to:

(i) the consistency and appropriateness of use of source data supplies by the expert.
(ii) the assumptions and methods used, if appropriate, and their consistency with the previous period.
(iii) the results of the expert's opinion in the light of the internal auditor's overall knowledge of the business and of the results of his audit procedures

The internal auditor should not, normally, refer to the work of an expert in the internal audit report. Such a reference can, however, be considered useful, in case of reporting in respect of cases such as material weaknesses or deficiencies in the internal control system or in such other cases where the internal auditor feels that such a reference would benefit the readers of the report. While referring to such work of the expert, the internal auditor should outline the assumptions, broad methodology and opinions of the expert.

However if the internal auditor thinks it appropriate to disclose the identity of the expert, he should obtain prior consent of the expert for such disclosure and obtain his written consent if such consent has not already been obtained.

****

Chapter 11
Audit Conclusion and Corrective Measures

The internal auditor's observations, findings on various points during the course of internal audit of the entity which are not in accordance with the policies and procedures of the entity or contravening the generally accepted business practices of the entity. Even some times cases of fraud , misappropriation etc. are also observed / established during the course of internal audit of the entity that need to be reported to the management of the entity.

The Observations paragraph should clearly mention the process name, significant observations, findings, analysis and comments of the internal auditor on the issues which were identified during the course of internal audit process and have bearing on the performance of the entity.

On the findings, observation or comments of internal audits of an entity, there is a need for corrective action on the part of the management (auditee). The Action Taken Report paragraph should be appended after the observations and findings and should include:

(i) Status of compliance/ corrective action taken/ being taken by the entity with respect to previous internal audit observations or current internal audit observations;
(ii) Status of compliance/ corrective action not taken by the entity with respect to previous internal audit observations or current internal audit observations and the reasons for non-compliance thereof; and
(iii) Revised timelines for compliance of all items in (ii) where no corrective actions have been taken till the date of the report.

The internal auditor's report in the Summary paragraph of should clearly point out the highlights of the internal audit findings, key issues and observations of concern, significant controls lapses, failures or weaknesses in the systems or processes, nonconformities, deviation from laid policies and procedures etc. which have effect on the financial or non-financial aspects of the entity.

Where the internal auditor has highlighted the significant controls lapses, failures or weaknesses in the systems or processes, nonconformities, deviation from laid policies and procedures and seeks action taken report on such issues and no suitable action is taken by the management of the entity, such points become audit conclusions.

****

Chapter 12
Report writing and audit reports

At the end of each audit internal auditors typically issue reports wherein they summarize their findings, recommendations, and any responses or action plans from management. An audit report should have an executive summary; findings specific issues or related recommendations or action plans; and appendix details comprising graphs and charts or process information.

The recommendations in an internal audit report are helpful for the organization to exercise effective and efficient governance, risk and control processes associated with operations objectives, financial and management reporting, legal/regulatory compliance and compliance of laid policies and procedures.

Audit observations and recommendations should relate to particular statements about transactions, such as whether the transactions audited were valid or authorized, properly processed, correctly valued, processed as per schedule, properly disclosed in financial or operational reporting and carried out as per the entity's policies and objectives.

Under the International Internal Auditing (IIA) standards, the preparation of a balanced report is a critical component of the audit process. The internal audit report provides executives and the board with the opportunity to assess and evaluate the issues being reported in the proper background and as a constructive approach. By providing suggestions, viewpoint, analysis and feasible recommendations for business improvements in vital and critical areas, auditors help the entity to achieve its targets and objectives.

The audit report shall have five elements, sometimes called the "5 C's":

1. **Condition:** What is the particular problem identified?
2. **Criteria:** What is the standard that was not met? The standard may be a company policy or other benchmark.
3. **Cause:** Why did the problem occur?
4. **Consequence:** What is the risk/negative outcome (or opportunity foregone) because of the finding?
5. **Corrective action:** What should management do about the finding? What have they agreed to do and by when?

Internal audit reporting

At the end of the audit an audit report containing a clear written expression of significant observations, suggestions/recommendations on the vital and critical areas is prepared. Such report should be based on the policies, processes, risks, controls and transaction processing taken into consideration and

managements' responses obtained during the course of audit.

The internal auditor's report includes the following basic elements:

(a) *Title of the report;*

(b) Addressee to whom the report is submitted;

(c) Period of coverage of the Report;

(e) Introductory or opening paragraph of the Report which deals with;

(i) Identification of the processes/functions and items of financial and non-financial statements audited;

(ii) A statement of the responsibility of the management of the entity and the responsibility and obligations of the internal auditor;

(f) Objectives paragraph of the Report – scope and coverage of the internal audit engagement;

(g) Scope paragraph of the Report (dealing with the nature of an internal audit):

(i) A reference to the applicable generally accepted internal audit procedures and standards;

(ii) A description of the engagement and the approach and methodology of the internal audit specifying procedures performed by the internal auditor; and

(iii) A description of the population sample for the audit and the sampling technique applied.

(h) Executive Summary, highlighting the key material issues, suggestions, observations, critical areas, control weaknesses in the system and exceptions;

(i) Observations, findings and recommendations;

(j) Comments/ responses from the management;

(k) Action Taken Report –pursuant to the observations made in the previous internal audit reports or observations when action not taken on issues reported.

(l) Date of the report;

(m) Place of preparation/ issue of the report;

(n) Authentication of the report;

(n) Internal auditor's signature with Membership Number

The internal auditor should take due professional care and apply professional skills to ensure that the internal audit report, inter alia, is:

(i) concise and clear

(ii) factual – presents all significant matters with disclosure of material facts

(iii) specific

(iv) unambiguous

(v) submitted as per the schedule

(vi) complies with applicable generally accepted internal audit standards and procedures.

The internal auditor's report should be appropriately addressed as required by the circumstances of the engagement. Ordinarily, the internal auditor's report is addressed to the appointing authority or such other person as directed.

Reporting of critical findings

Internal audit emphasized assisting management and the Board in achieving the organization's objectives through well-reasoned audits, evaluations, and analyses of operational areas. He encouraged the modern internal auditor to act as a counselor to management rather than as an adversary.

The internal auditor reports the observation, suggestions and recommendations on critical issues to the Board, the Audit Committee, and Executive Management or to such other person who is authorised to receive internal auditor's report along with management's progress towards resolving them. As certain most critical issues have a reasonable likelihood of causing substantial financial loss or reputational damage to the entity. It is a matter of considerable judgment to select flag issues which are critical and need Audit Committee's attention and to emphasize these issues in the proper context in the internal audit report.

Where the critical issues or weak areas are identified during the course of internal audit, the internal auditor should discuss such issues with the management before incorporating them in the in the report. Writing about positive observations in audit reports was rarely done however for building better relationships this should be done. In the audit report acknowledgment should be given for support and cooperation by entity (auditee).

****

Chapter 13

Introduction to Indian Telecom Sector

An Overview

Telecommunications has evolved as a basic infrastructure like electricity, roads, water etc. and has also emerged as one of the critical components of economic growth required for overall socio economic development of the country. The Indian telecom sector has registered a phenomenal growth during the past few years and has become second largest telephone network in the world, only after China. The Department of Telecommunications (DOT) under the Ministry of Communications and Information Technology was the monopoly agency providing communication facilities in India till 1994 when the first time private players were invited to contribute to the telecom sector by way of investment of providing telecom services in the country. Since then it has been one of the few sectors in India, which has witnessed widespread structural and institutional reforms.

Present Status

The Indian telecom network with 895.51 million telephone connections, including 864.72 million wireless telephone connections, at the end of December 2012 is second largest network in the world after China. Out of this, 338.59 million telephone connections are in rural areas and 556.92 million are in urban areas of the country. There were 24.01 million Internet subscribers including 14.68 million Broadband subscribers at the end of September 2012. The number of Broadband subscribers increased to 14.98 million, end of December 2012.

Present Status of the Telecommunication Sector (As on December 31, 2012)

- Indian telecom network is second largest in the world after China.
- The country has 895.51 million telephone connections, including 864.72 million wireless telephone connections.
- Overall tele-density in the country is 73.34%.
- Urban tele-density is 149.55%, whereas rural tele-density is 39.90%.
- The share of wireless telephones in total telephones is 96.56%.
- The share of private sector in total telephones is 85.51%.
- Number of Broadband connections is 14.98 million.

Source: Annual Report 2013 of Department of Telecommunications http://www.dot.gov.in

Telecom Policies

The first National Telecom Policy was announced by the Government in 1994 (NTP-94) with the objectives of providing telephone on demand, provision of world class services at reasonable prices and universal availability of basic telecom services to all villages. NTP-1994 recognized that the required resources for achieving these targets could not be made available only out of Government sources and private investment and involvement of the private sector was required to bridge the large resource gap.

While there were several achievements under the NTP 1994, some of the objectives could not be met. Acknowledging several changes both at the national and global scenario in the telecom sector; a New Telecom Policy- NTP-99 was announced by Government w.e.f. 1st April 1999. Licensing of all telecom services thereafter was to be under the policy framework of NTP-99, which sought to significantly redefine the competitive nature of the industry. The new policy lifted the restrictions on the number of service providers for the Basic Service Providers (BSPs) as well as the Cellular Mobile Service Providers (CMSPs) making it open for participation by all bidders who satisfied the conditions of the DoT. The new policy also required all operators who were under the fixed licence fee regime to migrate to a revenue sharing regime. In the revenue sharing model, the operators were required to pay a percentage of their Adjusted Gross Revenue (AGR) as annual license fee and spectrum usage charge to the Government. The percentage of revenue share depended on the service area* where they offered their services.

The Union Cabinet based on the recommendations of Group of Ministers (GoM) on Telecom matters constituted in September 2003 approved the policy for licensing of Unified Access Services. The GoM had considered the recommendations submitted by Telecom Regulatory Authority of India (TRAI) on 27 October 2003. The policy drew upon NTP-99. Through this approval, Cabinet besides, a number of other related decisions, charted the course to a Universal Licensing Regime. Guidelines for issue of licenses under UAS were issued on 11 November 2003 where after licences were issued only under UAS.

In April 2007, the DoT sought the opinion of the TRAI on some specific points including that of putting a cap on the number of access service providers in a service area, as radio frequency spectrum required for wireless services was not sufficient to meet the increasing demand from UAS Licensees. TRAI recommended (August 2007) that no cap be placed on the number of access service providers in any service area. TRAI in August 2007 also recommended that “a licensee using one technology may be permitted on request, usage of alternative technology and thus allocation of dual spectrum. However, such a licensee must pay the same amount of fee which has been paid by the existing licences using the alternative technology or which would be paid by the new licensee going to use that technology”.

National Telecom Policy-2012 (NTP-2012) has been announced with the primary objective of maximizing public good by making available affordable, reliable and secure telecommunication and broadband services across the entire country.

Highlights of National Telecom Policy-2012 (NTP-2012)

The Government approved National Telecom Policy-2012 (NTP-2012) on 31st May 2012 which addresses the Vision, Strategic direction and the various medium term and long term issues related to telecom sector. The primary objective of NTP-2012 is maximizing public good by making available affordable, reliable and secure telecommunication and broadband services across the entire country. The main thrust of the Policy is on the multiplier effect and transformational impact of such services on the overall economy. It recognizes the role of such services in furthering the national development agenda while enhancing equity and inclusiveness. Availability of affordable and effective communications for the citizens is at the core of the vision and goal of the NTP-2012. The Policy also recognizes the predominant role of the private sector in this field and the consequent policy imperative of ensuring continued viability of service providers in a competitive environment. Pursuant to NTP-2012, these principles would guide decisions needed to strike a balance between the interests of users/ consumers, service providers and government revenue.

The objectives of the NTP-2012, inter-alia, include the following:

- Provide secure, affordable and high quality telecommunication services to all citizens.
- Strive to create One Nation - One License across services and service areas.
- Achieve One Nation - Full Mobile Number Portability and work towards One Nation - Free Roaming.
- Increase rural tele-density from the current level of around 39 to 70 by the year 2017 and 100 by the year 2020.
- To recognize telecom, including broadband connectivity as a basic necessity like education and health and work towards 'Right to Broadband'.
- Provide affordable and reliable broadband-on-demand by the year 2015 and to achieve 175 million broadband connections by the year 2017 and 600 million by the year 2020 at minimum 2 Mbps download speed and making available higher speeds of at least 100 Mbps on demand.
- Provide high speed and high quality broadband access to all village panchayats through a combination of technologies by the year 2014 and progressively to all villages and habitations by 2020.
- Recognize telecom as Infrastructure Sector to realize true potential of ICT for development.
- Address the Right of Way (RoW) issues in setting up of telecom infrastructure.
- Mandate an ecosystem to ensure setting up of a common platform for interconnection of various networks for providing non-exclusive and non-discriminatory access.
- Enhanced and continued adoption of green policy in telecom and incentivize use of renewable

resources for sustainability.

- Achieve substantial transition to new Internet Protocol (IPv 6) in the country in a phased and time bound manner by 2020 and encourage an ecosystem for provision of a significantly large bouquet of services on IP platform.

Need for Internal Audit of Telecom Sector

Internal audit is a significant tool in evaluating the adequacy of system controls and points out the state of compliance with the applicable laws and regulations, policies and procedures and ensures risk management and promote efficiency. Telecom sector is also a fast developing infrastructure sector and playing a dominant role in the development and growth in the economy of India. Like all business entities there is a strong need for audit of business entities involved in telecom business mainly due to following factors:

(i) Understand the issues facing Telecom Sector Companies in the modern business world of communications.

(ii) Assess the risks associated with Telecom Sector Companies and the techniques for identifying and controlling such risks.

(iii) Explore the use of the most appropriate audit techniques to optimise coverage of Telecom Sector Companies.

(iv) Develop methodologies to ensure the adequacy of system controls operating and systems to ensure adequate internal control framework over financial reporting of Telecom Sector Companies.

(v) Effective review of the major operating functions in a Telecom Company and make practical and value add recommendations for improvement in the operation of such companies.

(vi) Ensure revenue assurance and compliance with the applicable laws and regulations, policies and procedures by the telecom companies.

The Regulatory Regime

Licence Requirement

The telecom industry is regulated by the Ministry of Communications and Information Technology, Government of India through the Telecom Regulatory Authority of India (TRAI), TRAI regulates the telecom business through licensing requirements. A telecom company can provide only those services and in such telecom circles, for which license has been granted. Any telecom operator intending to enter into telecom business has to fulfill the various license requirements.

1.2Areas of telecom companies that needs the Audit

Following are the areas that mainly need to be audited:

1. Audit and Verification of payment of Licence Fee and other dues to Telecom Companies on the AGR.
2. Audit requirements under the Reporting System on Accounting Separation Regulations, 2012
3. Audit of Call Data Records (CDRs) to assess / determine / verify Service Provider- wise Liability of Transit Carriage Charge.
4. Audit of Metering and Billing System of Telecom Service Providers.
5. Audit of Functional services

****

Chapter14

Special Transactions peculiar to Telecom industry

The telecom industry has witnessed a very fast growth in India in the last decade or so. The horizon for the range of telecom services has expanded multi-folds. The range of services includes:

- Voice services like landline, mobile, satellite and internet based, NSD, ILD
- Data services like leased lines, Wi-Fi
- Video conferencing services
- Cable TV, DTH and broadcasting services

The telecommunications business is tightly regulated by TRAI in India. This regulation relates to the type of different services that are allowed to be provided and the prices at which these services could be charged.

The transactions peculiar to the telecom industry could be as follows:

a) **Licensing** – the telecom business cannot be undertaken without obtaining the statutory licenses form the Government of India. The license is given for a certain period and the operations are limited to certain geographies called as circles. The license cost is amortised over the period of license.

b) **Revenue streams** – the revenue is earned from various service offered by the entity. These services could be listed as below:
   i. Revenue from voice calls (wired, mobile, WLL etc.)
   ii. Revenue from data transfer services (use of internet and mail services)
   iii. Revenue from value added services such as call waiting, call diverting, caller ID, call forwarding, alarms, SMS services etc.
   iv. Revenue from renting of towers
   v. Revenue from roaming facilities provided

c) **Infrastructure sharing** – the telecom industry earns revenue through the sharing of infrastructure with the other service providers. The assets that are commonly shared are the networks (used across different circles for roaming services), the tower facilities, inter-operator call sharing etc. This arrangement works based on the agreement between the different operators and poses some challenges in terms of revenue & cost recognition, risks of abuse, and fraud. The internal control process for these should be used to exercise control on these activities.

The internal auditor is advised to understand the specific telecommunication services provided by the client organisation and also grasp the meaning of some technical terms used in the industry. For the benefit of the reader some of these terms are given below:

- AGR (Adjusted Gross revenue) is the revenue as per books of accounts adjusted by prescribed factors to decide the share of Government.
- BTS (base transmission station) is the centre that encodes, encrypts, multiplexes, modulates and feeds the RF (Radio Frequency) signals.
- Intelligent Network for processing call controls via distributed network transfer points.
- ISDN (integrated Service Digital Network) allowing both voice and data transmittals simultaneously across the world using end-to-end digital connectivity.
- Mediation is a network device that facilitates the receipt & processing of signals, reformatting in to other formats to be sent for the purpose of billing & reporting.
- VPN (Virtual Private Network) works to secure private communication paths facilitating the data transfer safely.
- Call flow Process includes the setups for outgoing calls and incoming calls.

The understanding of the above would enable the internal auditor to carry the audit of transaction in the telecom company. The following is the checklist of special transactions to be taken care of in this case:

Compliance with regulatory requirements

- Licensing requirements covering the capital norms, net worth norms and foreign participation norms
- License period, licensed services and licensed circles
- Fees payable include the following:
  - Entry fee – a onetime fee
  - License fee – it's the revenue share payable quarterly at the prescribed rate on the AGR as explained above
  - Radio spectrum charges for allotment of the frequencies for the GSM and CDMA
  - There is interest and penalty payable on the late payment of the above fees
  - The Performance Bank Guarantee and Financial Guarantee has to be given

- Reporting compliances such as:
  - Quarterly audited financials & the license fee
  - Operator wise statement of interconnection usage charge payments
  - Annual reconciliation of gross revenue, adjusted gross revenue

- Compliance with the TRAI guidelines on the subscriber verification is mandatory, hence the internal control assessment becomes very crucial
- Penalty payable if the conditions for routing the calls through dedicated trunks for local calls, NLD and ILD calls are not complied with, hence the internal auditor should verify the interconnect bill or any notice received from other telecom company to verify if penalty applies
- Another important reporting compliance is the report to be submitted as per the Accounting Separation Regulation 2012. This report is like the segmental report where the classification required is based on types of license, geographical area, product/service network, network cost etc.

Operating activity audit for telecom companies

The telecom service provider business is characterised by a very wide variety of services, each of which may require separate set of inputs and processing. The services may be provided as a package to the customers, thus making it difficult to correctly allocate the revenue and costs to each component of the service type.

One of the very crucial factors involving the threat of operating loss is revenue leakage. The leakage could be owing to many reasons such as

- Prepaid Call Data Record (CDR) may get configured as postpaid CDR and call balance may not get reduced for the prepaid subscriber and the call is also not billed in case of a postpaid subscriber
- Prepaid calls may not be charged on 'real time' basis
- Technical faults may not generate the CDR
- Wrong tariff plan configurations

The internal auditor should verify the revenue assurance process employed by the company and the effectiveness thereof by looking at variations from the standards if any. The report that they could refer to is the 'error CDR report' generated by the system. It will have to be further analysed according to the reasons

The internal auditor should refer to the report generated on the accounting separation to get a fair idea on the operating efficiencies of the different services offered by the company. The analysis of the following ratios would assist in assessing the operational weaknesses & strength:

- The churn rate i.e. customers leaving for competitor
- Average revenue per user (ARPU)
- Revenue per minute

- Minutes billed to total minutes recorded

The technical operating performance could be judged by looking at the various parameters recommended by the TRAI. Some of the useful indicators would indicate the wastages and efficiencies as follows. The areas that cover various performance parameters are listed below:

- Network related parameters – network availability, accessibility, retention ability, point of interconnection congestion,
- Customer service quality parameters – metering & billing, response time, termination of service, service activation time, service restoration time

The internal auditor should assess the internal control system with regard to the above areas and obtain the data on the various parameters to draw conclusions by observing trend and then benchmarking with the industry averages. The benchmarking data can be easily obtained through the TRAI annual report on the performance indicators.

Some useful ratios

- Downtime at Base Transceiver Station
- Call drop rate
- Connection with good voice quality
- Call set up success rate
- Metering and billing credibility
- Percentage of faults reported and resolved
- Average time to repair
- Call completion rates
- Minutes of use (MOU)

Metering and billing system

The internal auditor should verify the documents to find out the following:

- Information about the tariff plan is communicated to the subscriber in advance and also on activation
- Charges for the value added services must be informed to the subscriber
- All charges to be consistent with the published tariff
- Payments by subscribers are credited to their account for both pre and post-paid within the time limit prescribed

- Notice to be given to subscriber for any restriction or ceasing of the service
- Documentation process for the identifying, investigating and dealing with billing complaints by the subscribers
- Reliability of total metering and billing performance to be within the prescribed tolerance
- Compliance report to be submitted by 30th June every year

The internal auditor should verify if that the audit by notified auditor has been carried out for metering and billing.

Assessment of frauds

The internal auditor should study the risks regarding possibility of fraud. These frauds could be categorised as:

- External frauds – connected with subscription through false documentation and intentional defaults in the bill payments. The internal auditor should check the internal controls to check if existing defaulters do not re-enter the system, evaluation of the credit rating & assigning credit limit, monitoring of high usage, monitoring of calls
- Frauds through illegal telephone exchanges through the use of VoIP and PSTNs resulting into routing the international calls as local call causing huge revenue loss. The internal auditor should assess the internal control system to identify the possibility
- Frauds by cloning of handsets and SIMs
- Credit card frauds
- Internal frauds by the dealers, wrong configuration in the operating systems

Revenue recognition

The revenue will be basically be from the call charges, national & international roaming, value added services, registration, processing & activation charges, infrastructure sharing charges for passive links & active links, interconnection usage charges such as access deficit, carriage and call termination.

The internal auditor should understand the process of how these revenues are generated, the relevant agreements entered and the basis for recognizing the revenue.

- Postpaid service revenue is recognised according to the various services e.g. the fixed charge is recognised based on the billing month, the call charges, SMS charges & value added services are recognised based on the actual amount utilized & billed.
- The prepaid revenue is recognised only on the activation of the SIM in the initial stage and then on the activation of the recharge voucher. The recharge voucher amount should be split

between the administration charges, service tax and the talk time.

- The internal auditor should verify the process of the billing and review the IT system to obtain the input data for billing and recognizing the revenue.

Internal audit of fixed assets

The assets peculiar to the telecom industry are the underground OFC, BTS towers, network cards, routers and other such equipment apart from the normal fixed assets like land & building, equipment, DG sets, air-conditioning, etc. The very high volume and complexity of the business require the IT systems and the equipment to be robust, up-scalable and flexible. As the pace of obsolescence is very fast, the internal auditor should verify the risks associated with the same. Internal Auditor has to see that there should be a sound fixed assets management particularly network assets is existed in the organization. Following are the critical areas relating to fixed assets management:

- The internal auditor should verify the policy for capitalization and amortization of the hardware, license fee and the software used by the company.
- The IT systems should be verified to assess the synchronization, sufficiency of information and security of information.
- Organization plan/ policies for disposal of retired and redundant assets.
- Review necessary insurance coverage's of assets.
- Whether automated systems to track assets existed in the organisation and resources provided are sufficient for control over fixed assets.
- Robust system for regular assessment of control environment for assets managed by third parties. Existence of robust plan in place to verify, track and manage transition to next generation networks.

****

Chapter15

Telecom services offered which are allowed by the Department of Telecommunications (DoT) and revenue share levies

Department of Telecommunications (DoT) deals with Policy, Licensing and Coordination matters relating to telephones, wireless, data, facsimile and telemetric services and other like forms of communications. Licensing is done by DoT for: -

a. Access services
b. Carrier services
c. Data services
d. Other services

1. Access Services:

Basic/ Unified Access Services (UAS) / Cellular Mobile Telephone Service (CMTS)

(i) Basic Telephone Service

Basic Telephone Service means the collection, carriage, transmission and delivery of voice or non-voice messages over the service providers (Licensee's) Public Switched Telephone Network (PSTN).

(ii) Unified Access Services (UAS)

Unified Access Services (UAS) means telecommunication service provided by means of a telecommunication system for the conveyance of messages through the agency of wired or wireless telegraphy. The Unified Access Services refer to transmission of voice or non-voice messages over LICENSEE's Network in real time only. SERVICE does not cover broadcasting of any messages voice or non-voice, however, Cell Broadcast is permitted only to the subscribers of the service. The subscriber (all types, pre-paid as well as post-paid) has to be registered and authenticated at the network point of registration and approved numbering plan shall be applicable. Unified Access Services Provider (UASP) means a service provider (Licensee) authorized to provide Unified Access Services under a Licence in a specified service area by DOT.

(iii) Cellular Mobile Telephone Service (CMTS)

Cellular Mobile Telephone Service (CMTS) means telecommunication service provided by means of a telecommunication system for the conveyance of messages through the agency of wireless telegraphy where every Message that is conveyed thereby has been, or is to be, conveyed by means of a telecommunication system which is designed or adapted to be capable of being used while in motion. The Cellular Mobile Telephone Service refers to transmission of voice or non-voice messages over

LICENSEE's Network in real time only. SERVICE does not cover broadcasting of any messages voice or non-voice, however, Cell Broadcast is permitted only to the subscribers of the service. The subscriber (all types, pre-paid as well as post-paid) has to be registered and authenticated at the network point of registration and approved numbering plan shall be applicable. Cellular Mobile Telephone Service Provider (CMSP) means a service provider (Licensee) authorised to provide Cellular Mobile Telephone Service under a Licence in a specified service area.

The Department of Telecommunications under the Ministry of Communications and Information Technology is empowered to give licences for telecom services in India under the provisions of Indian Telegraph Act, 1885 and Indian Wireless Telegraphy Act, 1933 and authorised to charge licence fee and spectrum usage charges. As per DOT's orders, the licence fee payable by various categories of licences for the year 2013-14 and onwards is summarized in Annexure-A.

(a) Licence Fee

Under the terms and conditions of Basic/ Unified Access Services (UAS) / Cellular Mobile Telephone Service (CMTS) Licence a uniform licence fee rate of 8% of Adjusted Gross Revenue (AGR) shall be applicable across all categories of service areas (i.e. 'Metro', 'A', 'B' and 'C' categories) of UASL/ CMTS/ Basic service licensees for the year 2013-14 and onwards as follows:

Category of service license	**Annual licence fee rate as % of 'AGR'**
	For the year 2013-14 and onwards
'Metro' and Category 'A'	8%
Category 'B'	8%
Category 'C'	8%

(b) Spectrum usage charges

In addition to spectrum auction price, Spectrum usage charges are payable as a percentage of AGR from CMTS (using GSM/ CDMA Technology) as per the rates notified by the Government from time to time.

The present spectrum usage charges as notified in the Guidelines for Auction and Allotment of Spectrum in 1800MHz, 900MHz and 800MHz bands vide DOT's letter No. 1010/4/2012-WF (Auction) dated 22nd January 2013, are mentioned below:

Schedule A: Charges for GSM operators (Applicable for 1800MHz, 900MHz Bands)		**Schedule B: Charges for CDMA operators (Applicable for 800MHz Band)**	
Spectrum Slabs	**% of AGR**	**Spectrum Slabs**	**% of AGR**

Schedule A: Charges for GSM operators (Applicable for 1800MHz, 900MHz Bands)		**Schedule B: Charges for CDMA operators (Applicable for 800MHz Band)**	
Up to 4.4 MHz	3%	Up to 5 MHz	3%
Up to 6.2 MHz	4%	Up to 6.25 MHz	4%
Up to 8.2 MHz	5%	Up to 7.5 MHz	5%
Up to 10.2 MHz	6%	Up to 10 MHz	6%
Up to 12.2 MHz	7%	Up to 12.5 MHz	7%
Up to 15.2 MHz	8%	Up to 15 MHz	8%

2. Carrier Services:

(i) National Long Distance (NLD) Service

"National Long Distance (NLD) Service" refers to the carriage of switched bearer telecommunication service over long distance network i.e., a network connecting different Short Distance Charging Areas (SDCAs). **"**National Long Distance Service Provider**"** (NLDO)is the telecom operator providing the required digital capacity to carry long distance telecommunication service within the scope of LICENCE for National Long Distance Service, which may include various types of tele-services defined by the ITU, such as voice, data, fax, text, video and multi-media etc.

The company is required to pay a processing fee along with the application of Rs. 15,000/. The company is required to pay one-time non-refundable Entry Fee of Rs 2.5 crores before the signing of the Licence. In addition to entry fee described above the uniform annual licence fee @ 8% of the Adjusted Gross Revenue (AGR) shall be levied on NLD service for the year 2013-14 and onwards.

(ii) International Long Distance (ILD) Service

International Long Distance (ILD) Service is a network carriage service (also called Bearer) providing International connectivity to the Network operated by foreign carriers. The ILD service provider is permitted full flexibility to offer all types of bearer services from an integrated platform. The ILD service providers will provide bearer services so that end-to-end tele-services such as voice, data, fax, video and multi-media etc. can be provided by Access Providers to the customers. Except GMPCS including through INMARSAT the ILD service providers are permitted to offer international bandwidth on lease to other operators. ILD service provider shall not access the subscribers directly (except for Leased Circuits/CUG) which should be through NLD service provider or Access Provider. However, the ILD service provider may access the subscribers directly only for provision of International Long Distance voice service through

Calling Cards only. The ILD Service Provider is permitted to provide international bandwidth on lease to Resellers who are issued license for 'Resale of IPLC' under Section 4 of Indian Telegraph Act, 1885.

The company is required to pay a processing fee along with the application of Rs. 50,000/-. The company is required to pay onetime non-refundable Entry Fee of Rs 2.5 crores before the signing of the Licence. In addition to entry fee described above the uniform annual licence fee @ 8% of the Adjusted Gross Revenue (AGR) shall be levied on ILD service for the year 2013-14.

3. Data Services:

Internet Service

"**Internet Service**" means all type of internet access or internet content services as provided in the Internet Service provider (ISP) Licence.

The uniform annual licence fee @ 8% of the Adjusted Gross Revenue (AGR) shall be adopted by all ISP and ISP-IT for the year 2013-14. Initially the validity period of ISP Licence was 15 years and entry fee was 20 lakh and 10 lakh for category 'A' & 'B' respectively but the guidelines dated 24.08.2007 have been amended w.e.f. 25.01.10 and validity period of new ISP licence (granted subsequent to 25.01.10) is 20 years with revised entry fee of Rs. 30 Lakh and 15 Lakh for category 'A' & 'B' respectively.

Subsequent to ISP Guidelines dated 24.08.07

Category	**Entry Fee Rs.**	**PBG Rs.**	**FBG Rs.**
A (All India)	30 Lakh	2 Crore	10 Lakh
B (a service Area out of 23 areas)	15 Lakh	20 Lakh	1Lakh

The applicant company (Licensee) is required to pay Rs. 15,000/- as processing fee along with the application for obtaining ISP Licence. Licensee having Net worth of Rs. 100 crore is eligible to take permission to provide Internet Protocol Television (IPTV) service.

4. Other Telecom Services

(i) Very Small Aperture Terminal (V-SAT)

"V-SAT" means Very Small Aperture Terminal. There are two types of CUG VSAT licenses: (i) Commercial CUG VSAT license and (ii) Captive CUG VSAT license. The commercial VSAT service provider can offer the service on commercial basis to the subscribers by setting up a number of Closed User Groups (CUGs) whereas in the captive VSAT service only one CUG can be set up for the captive use of the licensee.

A uniform annual licence fee rate of 8% of AGR shall be levied for all Commercial VSAT and MSS-R licences for the year 2013-14.

(ii) Public Mobile Radio Trunked Service (PMRTS)

Public Mobile Radio Trunked Service means service which is defined as (i) a two way land mobile service in which user communicate among themselves through a pair of radio frequencies out of a pool in a designated frequency band assigned to the system using (ii) the pair of radio frequencies is allocated on placement of call request and returned to the pool on the completion of the call (iii) the communication usually takes place through repeater station (also called base station) Once user is assigned channel(a pair of frequencies) by the system, no one else can interfere with the communication.

There shall be no entry fee. All PMRTS licensees including those using Captive Mobile Radio Trunked Service shall pay licence fee except for agencies working for public service such as Police, Fire and Government Security etc.

The uniform annual licence fee @ 8% of the Adjusted Gross Revenue (AGR) shall be levied on PMRTS service for the year 2013-14. There shall be separate charges (Royalty and Licence fee) for use of Radio Spectrum for commercial as well as captive system shall continue. This will be subject to changes made by Wireless & Planning Cell (WPC) of DOT from time to time.

(iii) Infrastructure provider category- II (IP- II)

"Infrastructure Provider**"** means a person or persons providing inactive elements of the telecom network including dark fibres, right of way, duct space, towers etc. as well as those who provide end-to-end bandwidth on a long-term basis. Infrastructure Providers Category-II (IP-II Licence) establishes as well as lease, rent out or sell digital transmission capacity (end–to-end bandwidth) capable to carry a message.

The applicant company is required to pay Rs. 10,000/- as processing fee along with the application. Infrastructure Providers Category-II are exempted from payment of entry fee as well as licence fee to the Licensor (DOT).

Annexure- A

As per DOT's orders, the licence fee payable by various categories of licences for the year 2013-14 and onwards: -

S. No.	Category of License	Revenue Share payable for the year 2013-14 and onwards
1	UASL/ CMTS/ Basic	**8% of AGR**
2	National Long Distance	
3	International Long Distance	
4	Internet without Telephony	
5	Internet with Telephony	
6	Commercial VSAT	
7	PMRTS	

****

Chapter 16
Concept of Revenue of a Telecom Service Sector Company and Levy of Licence Fee and other Dues

Under section 4 of the Indian Telegraph Act 1885, the Central Government has exclusive privilege of 'establishing, maintaining and working of telecommunication' and under the proviso of said section the Government has the right to transfer its privilege by way of Licence to any person on such conditions and for consideration of such payments, as it thinks fit. The source of power for granting Licence to provide telecom services and collecting licence fee is derived under the proviso to section 4 of the Indian Telegraph Act 1885. Telecom Licences to service providers are issued under the above provision and the Government is charging licence fee on the basis of revenue share. A fixed percentage of revenue shares is charged on the Adjusted Gross Revenue (AGR) of a particular type of telecom service for which Department of Telecommunications (DoT), Ministry of Communications and Information Technology, Government of India has issued the Licences to the telecom service providers to provide various types of telecom services in India.

Based on the telecom licence service for which DoT has issued the Licence a specified percentage of Adjusted Gross Revenue (AGR) is charged as s licence fee from the telecom service provider on quarterly basis. The concept of revenue recognition of telecom service provider is based on the same principle which is applicable to all business entities in the country.

The concept of revenue recognition under various jurisdictions:

(i) As per the definition given in Indian Accounting Standard (AS-9), the term revenue is explained as under:

"Revenue is the gross inflow of cash, receivables or other consideration arising in the course of the ordinary activities of an enterprise from the sale of goods, from the rendering of services, and from the use by others of enterprise resources yielding interest, royalties and dividends. Revenue is measured by the charges made to customers or clients for goods supplied and services rendered to them and by the charges and rewards arising from the use of resources by them. In an agency relationship, the revenue is the amount of commission and not the gross inflow of cash, receivables or other consideration"

(ii)

(iii) The Part-II of the revised schedule VI of the Companies Act, 1956 prescribes the method of presentation of revenue and its disclosures in the Profit & Loss statement of a company. As per this schedule the revenue should be presented on the face of Profit & Loss Statement as under:

I. Revenue from operations

II. Other income

III. Total Revenue (I + II)

Further, Note 2(A) to General Instructions for the Preparation of Statement of Profit and Loss requires that in respect of a company other than a finance company, revenue from operations is to be separately disclosed in the notes, showing revenue from:

(a) Sale of products
(b) Sale of services
(c) Other operating revenues
d) Less: Excise duty

As per Note 4 to General Instructions for the Preparation of Statement of Profit and Loss, Other income should be classified as:

(a) Interest Income (in case of a company other than a finance company);
(b) Dividend Income;
(c) Net gain/loss on sale of investments
(d) Other non-operating income (net of expenses directly attributable to such income).

(iv) The Ministry of Corporate Affairs has notified Ind AS in February 2012 which is converged on the lines of IFRS. Ind AS –on "Revenue" defines the revenue as under:
"Revenue is the gross inflow of economic benefits during the period arising in the course of the ordinary activities of an entity when those inflows result in increases in equity, other than increases relating to contributions from equity participants.

Revenue includes only the gross inflows of economic benefits received and receivable by the entity on its own account. Amounts collected on behalf of third parties such as sales taxes, goods and services taxes and value added taxes are not economic benefits which flow to the entity and do not result in increases in equity. Therefore, they are excluded from revenue. Similarly, in an agency relationship, the gross inflows of economic benefits include amounts collected on behalf of the principal and which do not result in increases in equity for the entity. The amounts collected on behalf of the principal are not revenue. Instead, revenue is the amount of commission".

(v) The International Accounting Standards Board has issued IAS/IFRS which are globally accepted standards of accounting. IAS-18 on 'Revenue' defines Revenue as:
'*Revenue includes only the gross inflows of economic benefits received and receivable by the entity on its own account. Amounts collected on behalf of third parties such as sales taxes, goods and services taxes and value added taxes are not economic benefits which flow to the entity and do not result in increases in equity. Therefore, they are excluded from revenue. Similarly, in an agency relationship, the gross inflows of economic benefits include amounts collected on behalf of the principal and which do not result in increases in equity for the entity. The amounts collected on behalf of the principal are not revenue.*

Instead, revenue is the amount of commission"

Determination of Gross Revenue (GR) and Adjusted Gross Revenue (AGR) in Telecom Sector in India

The definition of Gross Revenue (GR) and Adjusted Gross Revenue (AGR) adopted in the Licences by the DoT is broadly the same across all services. The gross revenue is revenue derived from providing licensed service/ accruing to the licensees, revenue on account of interest, dividend, value added services, supplementary services, roaming charges, late fees etc. For the purpose of License fee, Gross Revenue is adjusted for certain pass through items like (i) Public Switched Telecom Network (PSTN) related call charges actually paid to other service providers within India, (ii) roaming revenue on account of revenue charges actually passed to other service providers and service tax actually paid to Government to arrive at AGR.

The components of GR and the list of pass through items being deducted from GR to arrive at AGR for the purpose of licence fee under the different licence agreement for different kinds of telecom services are given below:

Name of Service	**Gross Revenue as per license agreement**	**Items to be deducted to calculate Adjusted Gross revenue**
Unified Access Service Licence (UASL)	The Gross Revenue shall be inclusive of installation charges, late fees, sale proceeds of handsets (or any other terminal equipment etc.), revenue on account of interest, dividend, value added services, supplementary services, access or interconnection charges, roaming charges, revenue from permissible sharing of infrastructure and any other miscellaneous revenue, without any set-off for related item of expense, etc.	(i) PSTN related Call charges (access charges) actually paid to Bharat Sanchar Nigam Ltd. (BSNL) / Mahanagar Telephone Nigam Ltd. (MTNL) or other telecom service providers within India. (ii) Roaming revenues actually passed on to other telecom service providers, and (iii) Service Tax on provision of service and Sales Tax actually paid to the Government; if gross revenue had included the component of Service Tax.
CMTS	The Gross Revenue shall be inclusive of installation charges, late fees, sale proceeds of handsets (or any other terminal equipment etc.), revenue on account of interest, dividend, value added services, supplementary services, access or interconnection charges, roaming charges, revenue from permissible sharing of	(i) PSTN related Call charges (access charges) actually paid to Bharat Sanchar Nigam Ltd. (BSNL) / Mahanagar Telephone Nigam Ltd. (MTNL) or other telecom service providers within India. (ii) Roaming revenues actually passed on to other telecom service providers, and

	infrastructure and any other miscellaneous revenue, without any set-off for related item of expense, etc.	(iii) Service Tax on provision of service and Sales Tax actually paid to the Government; if gross revenue had included the component of Service Tax.
BASIC	The Gross Revenue shall include all revenues accruing to the licensee on account of goods supplied, services provided, leasing of infrastructure, use of its resources by others, application Fee, installation charges, call charges, late Fees, sale proceeds of instruments (or any terminal equipment including accessories), handsets, band width, income from Value Added Services, supplementary services, access or interconnection charges, roaming charges, any lease or rent charges for hiring of infrastructure etc. and any other miscellaneous items including interest, dividend etc. without any set off of related items of expense, etc.	(i) PSTN related call charges (access charges) actually paid to other telecom service providers for carriage of calls; (ii) service tax for provision of service and sales tax actually paid to the Government, if gross revenue had included the component of service tax.
NLD	'Gross Revenue" the revenue income accruing to the licensee by way of providing NLD service under the licence including the revenue on account of supplementary/value added services and leasing of infrastructure, interest, dividend etc. The Gross Revenue shall also include previous debits (e.g. bad debts recovered, of excess provisions in earlier years.) It is clarified that any lease or rent charges for hiring of infrastructure shall not be so deducted. Service tax and sales tax collected and passed on to the Government(s) from customers of the licensee shall not form a part of the Revenue.	"Component part of a pass-through nature payable to other service providers to whose networks the Licensee's NLD network is interconnected for carriage of calls.

ILD	The Gross Revenue shall include all revenues accruing to the licensee on account of goods supplied, services provided, leasing of infrastructure, use of its resources by others, application Fee, installation charges, call charges, late fees, sale proceeds of instruments (or any terminal equipment including accessories), handsets, band width, income from Value Added Services, supplementary services, access or interconnection charges, any lease or rent charges for hiring of infrastructure etc. and any other miscellaneous items including interest, dividend etc. without any set off of related items of expense, etc.	"Call charges (access charges) actually paid to other telecom service providers for carriage of calls; service tax for provision of service and sales tax actually paid to the Government, if gross revenue had included the component of service tax.
ISP	The Gross Revenue shall be inclusive of revenue from Internet access service, revenue from internet contents, revenue from Internet Telephony service, revenue from activation charges, revenue from sale, lease or renting of bandwidth, links, R&G cases, Turnkey projects etc., revenue from IPTV service, late fees, sale proceeds of terminal equipments, revenue on account of interest, dividend, value added services, supplementary services, interconnection charges, roaming charges, revenue from permissible sharing of infrastructure and any other miscellaneous revenue, without any set-off for related item of expense etc.	(i) Charges from pure Internet service, activation charges from pure internet subscribers. Pure Internet Services shall mean any method / device / technology to provide access to Internet unless explicitly prohibited and all content available including web-hosting, web-collocation which is available on internet without access restriction. (ii) Service Tax on provision of service and Sales Tax actually paid to the Government if gross revenue had included as component of Sales Tax and Service Tax. (iii) Roaming revenue actually passed on to other eligible/entitled telecom service provider.

Total revenue of the company vs. revenue from License activities:

It is always not possible that the total revenue shown in the Profit & Loss Statement of a company will match with the total revenue (AGR) calculated for the purpose of license fee. There may be a variance in

the figures of total revenue reported in the financial statements and those calculated for AGR. This may be due to the following:

i. The license fee is levied on AGR generated by each circle. A company may have more than one circle/area of operation and there is possibility of inter -circle transactions related revenue. These inter-circle revenue transactions are eliminated while calculating total revenue for reporting in the financial statements.

ii. Where a company is engaged in other business in addition to providing telecom services, the total revenue of the company depicted in the profit & Loss account will include revenue from all business of the company including telecom services.

In nutshell, the telecom companies (called Licensees) are required to pay a specified percentage of Adjusted Gross Revenue (AGR) as licence fee to the DOT9 called Licensor) in respect of each licensed service which is computed as per the format of Adjusted Gross Revenue (AGR) as Licence Fee prescribed in the Licence Agreement applicable to that particular service. A specimen of the format of Adjusted Gross Revenue (AGR) as Licence Fee prescribed in Unified Access Service Licence (UASL) Agreement is annexed.

ANNEXURE-

Format of Statement of Revenue and Licence Fee prescribed under Unified Access Services (UAS) Licence Agreement to Determine GR, AGR and Licence Fee from the Revenue records of the Telecom Service Provider

Format of Statement of Revenue and Licence Fee

_____(Name and address of operator)

Unified Access Services in_____(Service Area)

Statement of Revenue and Licence Fee for the Quarter ……

of the financial year……..

(AMOUNT IN RUPEES)

S.N.	PARTICULARS	ACTUALS FOR THE PREVIOUS QUARTER	ACTUALS FOR THE CURRENT QUARTER	CUMULATIVEUPTO THECURRENTQUARTER.
1	**Revenue from services**			
A	**Revenue from wireline subscribers:**			
(i)	Rentals			
(ii)	Call revenue within service area			

(iii)	National LONG DISTANCE CALL revenue			
(iv)	International LONG DISTANCE CALL revenue			
(v)	Pass thru revenue for usage of other networks (give OPERATOR-wise details)			
(vi)	Service tax			
(vii)	Service charges			
(viii)	Charges on account of any other value added services, Supplementary Services etc.			
(ix)	Any other income / miscellaneous receipt from wireline subscribers.			
B	**Revenue from WLL subscribers : (Fixed)**			
(i)	Rentals			
(ii)	Call revenue within service area			
(iii)	National LONG DISTANCE CALL revenue			
(iv)	International LONG DISTANCE CALL revenue			
(v)	Pass thru revenue for usage of other networks (give OPERATOR-wise details)			
(vi)	Service tax			
(vii)	Service charges			
(viii)	Charges on account of any other value added services, Supplementary Services etc.			
(ix)	Any other income / miscellaneous receipt from WLL subscribers.			
C	**Revenue from WLL subscribers : (handheld)**			

(i)	Rentals			
(ii)	Call revenue within service area			
(iii)	National LONG DISTANCE CALL revenue			
(iv)	International LONG DISTANCE CALL revenue			
(v)	Pass thru revenue for usage of other networks (give OPERATOR-wise details)			
(vi)	Service tax			
(vii)	Service charges			
(viii)	Charges on account of any other value added services, Supplementary Services etc.			
(ix)	Any other income / miscellaneous receipt from WLL subscribers.			
D	**Revenue from Mobile Services:**			
D (a)	**Revenue from GSM and 3G spectrum based Mobile Services:**			
D(a) 1.	**Post paid options:**			
i.	Rentals			
Ii	Activation Charges			
iii.	Airtime Revenue			
iv.	Pass through charges (provide operator-wise details)			
v.	Service Tax			
vi.	Roaming charges			
Vii	Service charges			
viii.	Charges on account of any other value added services. Supplementary Services etc.			
ix.	Any other income/ miscellaneous receipt from post paid options.			
D(a) 2.	**Pre-paid options:**			

i.	Sale of pre-paid SIM cards including full value of all components charged therein.			
ii.	Any other income/ miscellaneous receipt from pre-paid options.			
D(a) 3. i.	**Revenue from Mobile Community phone service including full value of all components charged therein.**			
ii.	**Any other income/ miscellaneous receipt from Mobile Community phone service.**			
D (b)	**Revenue from CDMA based Mobile Services:**			
D(b) 1.	**Post paid options:**			
i.	Rentals			
Ii	Activation Charges			
iii.	Airtime Revenue			
iv.	Pass through charges (provide operator-wise details)			
v.	Service Tax			
vi.	Roaming charges			
Vii	Service charges			
viii.	Charges on account of any other value added services. Supplementary Services etc.			
ix.	Any other income/ miscellaneous receipt from post paid options.			
D(b) 2.	**Pre-paid options:**			
i.	Sale of pre-paid SIM cards including full value of all components charged therein.			
ii.	Any other income/ miscellaneous receipt from pre-paid options.			

D(b) 3. i.	**Revenue from Mobile Community phone service including full value of all components charged therein.**			
ii.	**Any other income/ miscellaneous receipt from Mobile Community phone service.**			
D (c)	**Revenue from BWA Services:**			
D(c) 1.	**Post paid options:**			
i.	Rentals			
Ii	Activation Charges			
iii.	Airtime Revenue			
iv.	Pass through charges (provide operator-wise details)			
v.	Service Tax			
vi.	Roaming charges			
Vii	Service charges			
viii.	Charges on account of any other value added services. Supplementary Services etc.			
ix.	Any other income/ miscellaneous receipt from post paid options.			
D(c) 2.	**Pre-paid options:**			
i.	Sale of pre-paid SIM cards including full value of all components charged therein.			
ii.	Any other income/ miscellaneous receipt from pre-paid options.			
D(c) 3. i.	**Revenue from Mobile Community phone service including full value of all components charged therein.**			
ii.	**Any other income/ miscellaneous receipt from Mobile Community**			

	phone service.			
E	**Revenue from Voice Mail /any other value added service**			
2	**Income from trading activity (all including of sales tax)**			
(i)	Sale of handsets			
(ii)	Sale of accessories etc.			
(iii)	Any other income/ miscellaneous receipt from trading activity.			
3	**Revenue from roaming.**			
i.	Roaming facility revenue from own subscribers.			
ii.	Roaming revenue from own subscriber visiting other networks including STD/ISD/pass thru charges for transmission of incoming call during roaming.			
iii.	Roaming Commission earned.			
iv.	Roaming revenue on account of visiting subscribers from other networks (provide operator-wise details).			
v.	Service Tax if not included above.			
vi.	Any other income/miscellaneous receipt from roaming.			
4	**Income from investments**			
(i)	Interest income			
(ii)	Dividend income			
(iii)	Any other miscellaneous receipt from investments.			
5	**Non-refundable deposits from**			

	subscribers			
6	**Revenue from franchisees /resellers including all commissions and discounts etc. excluding the revenues already included in IA&IB**			
7	**Revenue from sharing/ leasing of infrastructure**			
8	**Revenue from sale/ lease of bandwidth, links, R&G cases, turnkey projects etc.**			
9	**Revenue from other OPERATORs on account of pass through call charges** (provide operator-wise details)**.**			
10	**Revenue from other OPERATORs on account of provisioning of interconnection** (provide operator-wise details)			
11	**Miscellaneous revenue**			
AA	**GROSS REVENUE OF THE LICENSEE COMPANY: (Add 1-11)**			
BB	**DEDUCT:**			
1	Charges actually paid to other SERVICE PROVIDER(s) (OPERATOR-wise)			
2	Roaming revenues actually paid to other CMSPs And GMPCS service			

	providers. (operator-wise)			
3	Service Tax paid to the Government			
4	Sales Tax paid to the Government			
BB	**TOTAL DEDUCTIBLE REVENUE (1+2+3+4)**			
CC	**ADJUSTED GROSS REVENUE (AA-BB)**			
	REVENUE SHARE @ ---------- OF ADJUSTED GROSS REVENUE			

Format of Auditor's Report On Statement Of Revenue And Licence Fee

To

The Board of Directors

…….

…….

We have examined the attached Statement of Revenue and Licence Fee of ……(the name of the operators) for the quarter(s) ending _____. We have also examined the reconciliation of the cumulative figures for the quarter(s) ending _____ appearing in the Statement of Revenue and Licence Fee of the company with the figures appearing in the profit and loss account of the company for the year ended_____ which was audited by us. We understand that the aforesaid statement(s) (and the reconciliation) is /are to be furnished to the Central Government for assessment of the Licence fee payable by the company to the Government, in terms of the Licence agreement No……. signed between the company and the Department of Telecommunications.

We report that:

1. We have obtained all the information and explanations which to the best of our knowledge and belief were necessary for the purposes of our audit.
2. In our view, the company has an adequate internal control system in relation to revenues which is commensurate with its size and the nature of its business. The system, in our opinion, provides reasonable assurance that there is no unrecorded revenue and that all revenue is recorded in the proper amount and in the proper period.
3. No amounts payable in respect of sales tax, service tax or PSTN/toll/roaming charges were outstanding at the last day of the quarter(s) for a period of more than two months from the date they became payable, except for the following:……

4. In our opinion and to the best of our knowledge and belief and according to the explanations given to us, the Statement has been prepared in accordance with the norms/guidelines contained in the said Licence agreement in this behalf and gives a true and fair view of the revenue and Licence fee payable for the period computed on the basis of the aforesaid guidelines except for the following:

* Strike off wherever not applicable.

(SIGNATURE)

****

Chapter 17
Audit requirements under the Reporting System on Accounting Separation Regulations, 2012 issued by TRAI

1. Applicability for Filing of ASR Audit Report

These regulations shall apply to all service providers having aggregate turnover of not less than rupees one hundred crore, during the accounting year for which report is required to be submitted under these regulations, from operations under the licence issued under section 4 of the Indian Telegraph Act, 1885.

2. Telecom Services for ASR regulation

S. No.	Name of Telecom Service	Geographical area of Operation
1	Access Service - Wireless (Full Mobility)	Telecom Circle
2	Access Service – WLL	Telecom Circle
3	Access Service – Wireline	Telecom Circle
4	Internet Service	All India
5	National Long Distance	All India
6	International Long Distance	All India
7	Tower Business	All India
8	Dark Fibre	All India
9	Cable Landing Station	All India
10	Mobile Number Portability (MNP)	All India
11	Very Small Aperture Terminal Service (VSAT)	All India

3. Reports

Every service provider shall furnish to the Authority the financial and non-financial reports:

(a) every accounting year based on Historical Cost Accounting for all the services specified in above table and;

(b) every second accounting year based on Replacement Cost Accounting for the following services namely :

(i) Access Service – Wireless (Full Mobility)
(ii) Access Service – WLL
(iii) Access Service – Wireline
(iv) National Long Distance Service
(v) International Long Distance Service

Provided that a service provider is not required to furnish the Accounting Separation Reports based on Replacement Cost Accounting for three years from the date of issue of licence.

4. ASR Audit report includes 10 Proformae which is defined below :

S. No.	Proforma	Description of the Proforma
1	Proforma A	Profit and Loss Statement – Service
2	Proforma B	Profit and Loss Statement – Product
3	Proforma C	Cost Sheet - Network Elements
4	Proforma D	Cost Sheet - Support Functions/Departments
5	Proforma E	Statement of Gross Block, Depreciation and Net Block – Service
6	Proforma F	Capital Employed Statement- Service
7	Proforma G	Capital Employed Statement: Allocation to Products
8	Proforma H	Statement of Related Party Transactions
9	Proforma I	Reconciliation Statement (covering all services and area of operations) with Audited Financial Statements.
10	Proforma J	Statement of Non-financial information for each service

5. Approval from of Board of Directors

a) The accounting separation reports prepared by the service provider under regulation 4 of Regulations shall be adopted by the Board of Directors of the company and shall be signed by the authorized signatory before submitting the same to Auditor.

b) The accounting separation reports prepared by the service provider and the audit report shall be signed by the auditor or a partner of the firm, if a firm is appointed as auditor.

6. **Submission of ASR audit report**

a) The accounting separation reports along with the audit report shall be submitted to the TRAI within 6 months of the close of the accounting year.

b) The reports shall be submitted in hard copy and in soft copy in MS Excel format along with its formulae and linkage.

c) Every service provider shall for the purpose of implementing the accounting and reporting practices specified under these regulations furnish to the Authority within 90 days from the date of commencement of these regulations, a manual containing policies, principles, methodologies and procedures for accounting and cost allocation

****

Chapter 18

Audit of Call Data Records (CDRs) to assess / determine / verify Service Provider- wise Liability of Transit Carriage Charge

1. Need for Audit of CDRs: Consequent upon the issue of an Order or Direction or Regulation issues by the Telecom Regulatory Body, the auditors / consultants are required to analyse / audit the Call Data Records (CDR) of the telecom service providers which are providing Access Service (Basic (Wireline) and Cellular Mobile (Wireless) Service to the customers in India needs to be audited to verify the Carriage Transit Charges (part of Interconnection Usage charges (IUC)) to assess the liability of the Telecom Service Providers towards such charges towards the Carriage Transit facility provider.

Call Data Record (CDR) contains the record of the details of the call made by the customer of one telecom service provider to the customer of other telecom service provider using the telecom network of such other telecom service provider to carry or terminate (or both) the call. Usual information on a CDR includes date, start time of call, end time of call, duration of call, originating number and terminating number. Call Data Record (CDR) details is used to determine the transit carriage charges which are the charges to be paid by one cellular operator to other operator for carriage of intra-circle mobile traffic handed over by UASL/CMTS networks to Fixed network of other operator, at Level II Trunk Automatic Exchange (TAX) of Long Distance Charging Area (LDCA) in which the call is to be terminated, to the Short Distance Charging Area (SDCA).

2. Auditor 's role, responsibilities and scope of work for analysis of CDRs:

(i) To assess and verify the liability of each telecom service provider as per the Order / Direction or Regulation issues by the Telecom Regulatory Body. Therefore, in order to assess and verify the liability in terms of transit carriage charges, the distance slabs will be taken into consideration as per the carriage charges as specified in the Telecommunication Interconnection Usage Charges (IUC) Regulation issued by the Telecom Regulatory Authority. The assessment and verification of the liability in terms of transit carriage charges can be carried out as per the per minute rate specified in the Telecommunication Interconnection Usage Charges (IUC) Regulation issued by the Telecom Regulatory Authority or such other rate which have been agreed upon by the service provider as per Interconnection Agreement among them.

The verification of call data of service providers can be done on the basis of call data maintained by both the telecom service providers will be considered as parent data.

The Auditor will assess or determine/ verify service providers-wise, service area-wise and month-wise liability of each service provider in terms of transit carriage charges and report in the prescribed format as per the requirement of the Order / Direction or Regulation issues by the Telecom Regulatory Body. The report should contain observations and recommendation also include the summary and explanation of the analysis of CDRs in the report format, if any prescribed.

****

Chapter 19
Audit of Metering and Billing System of Telecom Service Providers

1. **Need for Audit:** The Telecom Regulatory authority receives billing related complaints for the telecom customers, consumer advocacy groups (CAGs) and by any other consumer welfare association. The complaints are mainly related to lapses with regard to flaws in billing system, configuration of systems in accordance with the applicable Tariff Plan, wrong billing due to linking of wrong Tariff Plan, malfunctioning of software of the Telecom Service Providers due to which the customers are wrongly billed by the Telecom Service Providers. Through the implementation of Regulation the Telecom Regulatory Authority ensures that telecom service provider is generating correct bills to the customers. To ensure this the Telecom Regulatory Authority gets conducted the audit of the telecom service provider based on the parameters with benchmarks for fair and reliable metering and billing system by notifying the Quality of Service (Code of Practice for Metering and Billing Accuracy) Regulation 2006 dated 21st March 2006 and subsequently amended Regulation vide notification dated 25th March 2013.

2. **System of appointment of auditors for metering and billing audit:** The Quality of Service (Code of Practice for Metering and Billing Accuracy) Regulation 2006 and subsequently amended Regulation vide notification dated 25th March 2013 has a provision that the Telecom Regulatory Authority should notify a panel of auditors to audit the Metering and Billing System of service providers. The service providers may appoint any one of these Auditors for auditing their billing system vis-à-vis the Code of Practice for metering and billing accuracy.

3. **Role and duties of Auditors:** The Auditors shall assess Service Providers' Metering and Billing System and approve compliant Service Providers' Metering and Billing System in accordance with the Quality of Service (Code of Practice for Metering and Billing Accuracy) Regulation 2006 as amended. The Auditors shall perform the audit to check compliances of the service provider to the code of practice for metering and billing accuracy laid down in the aforesaid Regulations.

4. **Areas of concern for auditors:**

(i) *Non-Compliance* ~ an instance of failure to comply with an established requirement. The nature of the failure and the requirement in question need to be made explicit in documenting any Non-Compliance.

(ii) *Deficiency* ~ an instance of a lack of adequacy in meeting a requirement. An example might be where a Billing system has no facility to detect duplication of records for the same Service Usage.

This would be likely to lead to a breach of Code of Practice for Metering and Billing Accuracy, but the absence of a detection facility only causes a problem when such duplication occurs.

(iii) *Observation* ~ a comment about something that has been seen during an assessment, but is not considered sufficiently serious to be a Deficiency. However, it may possibly lead to corrective and / or preventative action.

5. Audit areas, audit checks and procedure: The auditors have to undertake:

A. the verifications of billing and charging of telecom operators both for prepaid and postpaid customers in accordance with the Code of Practice for Metering and Billing Accuracy in a representative manner within the overall sample size.

B. the auditors have to specifically evaluate inter alia the correctness of the following: -

- generation process of the Call Data Records (CDR) - raw CDRs.
- the entries in the direction table which is used for rating the raw CDRs.
- the rated CDR vis-à-vis the rate applied, duration mentioned, origination and destination codes.
- charging of VAS services to the subscribers.
- charging of the roaming services to the mobile subscribers.

C. The tariff plans having subscribers more than 10 % of the total subscribers will be audited in each licensed service area. The number of sample size to be checked in each tariff plan so that the verification should be such so as to achieve a confidence level of 95% at a confidence interval of 3%.

D. Audit Agency will take the raw CDRs post-mediated and unrated & process the same to generate the Bill and then verify with already generated bill for any discrepancy. The CDRs of last three months are to be processed. In all cases metering and mediation process to be checked first by sample test calls to ascertain that metering and mediation process is accurate and no systemic deficiency is noticed. After doing the functional testing of the mediation process/software, unrated post-mediated CDRs may be used for generating the bills for audit analysis.

E. In the case of Prepaid, rated CDRs are produced by the IN system. In the absence of any un-rated CDRs, sample test calls shall be made using test SIM Cards/ telephone for every possible charge scenario and corresponding accuracy of rating procedures by the IN system may be established. Backward reconciliation of rated CDRs from IN system shall be done to further establish correctness of rating procedures.

An illustrative audit check list for Metering & Billing Audit is annexed.

6. **Audit Reporting:** Auditor shall prepare an Audit Report in accordance with the following:
   - Details of tariff plans audited;
   - Separate audit report for each of the licensed service area (area of operation of the telecom service provider for which Auditor has been engaged by the telecom service provider;
   - The detailed methodology for carrying out the System Audit.
   - Comments on compliance, deficiency or an observation with respect to each of the code /quality parameter laid down in the Code for Practice for metering and billing accuracy;
   - Certification that he has received all information and explanation from the service provider, necessary for the purpose of audit;
   - Comments of the Auditor about authenticity of the information received from the service provider for carrying out the Audit.

7. **Qualification of Auditors:** The Auditor should have accreditation from the Quality Council of India/ National Accreditation Board for Certification Bodies or from the International Accreditation Forum or should be an audit firm registered with the Institute of Chartered Accountants of India/ Institute of Costs and Works Accountants of India having experience in technical audit of similar nature to carry out the Metering and Billing approval process as defined in the Quality of Service (Code of Practice for Metering and Billing Accuracy) Regulation 2006 as amended from time to time by the Telecom regulatory authority. The Auditor should preferably be qualifies as system auditor or have proven experience in the audit of Billing System / Credit Card System / Prepaid Billing System besides having expertise of understanding of software relating to telecommunication / communication system & technology / Information Technology (IT).

8. **Independence of auditors:** The Auditors must be independent of Telecom Service Providers and avoid direct involvement in the design, construction, operation or maintenance of electronic communications networks or communications metering and / or billing solutions. They shall not represent parties engaged in these activities.

Annexure

Audit Check list for Audit of Metering and Billing System of Telecom Service Providers

Sr. No	Audit Area (item name)	Test to be performed
1	**Information relating to Tariffs**	
1.1	Before a customer is enrolled as a subscriber of any telecommunication service, he shall be provided in advance with detailed information relating to the tariff for using that service, in accordance with TRAI's Direction No.301-26/2003- TRAI(Eco) dated 2nd May, 2005 and No.301-49/2005-Eco dated 16.09.2005. Further, the service provider should inform the customer in writing, within a week of activation of service, the complete details of his tariff plan. Such information shall be in the format "C" prescribed in TRAI Direction No.301-26/2003-TRAI (Econ.) dated 2nd May, 2005. In addition, the following information shall also be provided: ▪ Quantity related charges (e.g. the charge for each SMS message, or kilobyte of data transmitted). ▪ Accuracy of measurement of time, duration and of quantity, and also the resolution and rounding rules, including the underlying units, used when calculating the charges for an individual event or an aggregation of events ▪ Contractual terms and conditions for supply, restriction and cessation of Service	▪ Verify the process for enrolment of a customer and check whether he was given information relating to tariff ▪ Verify whether the customer has been notified the complete details of tariff in writing within a week of activation (take sample cases and test check) ▪ Verify availability of information in tariff plan ▪ Verify accuracy of measurement and rounding rules.

Sr. No	Audit Area (item name)	Test to be performed
	▪ The service providers shall intimate a postpaid customer in advance about his credit limit. This information should also be available in the monthly statement/ bill of the customer on a regular basis. Service shall not be discontinued as long as the amount due is below the amount and his security deposit or the specified limit whichever is higher. TRAI Direction dated 27.06.2005 and 07.06.2006 refers. ▪ The service provider cannot increase tariff on any item within six months of enrolment in a tariff plan. Telecommunication Tariff Order (31st amendment) notified on 07.07.2004 refers. ▪ The customer is free to move from one tariff plan to another without paying any fee for migration.	▪ Verify contractual terms and conditions with reference to bill printed. ▪ Verify the process of intimating credit limit to subscribers. Check for instances where connections have been de-activated on the ground of the subscriber exceeding credit limits. ▪ Verify from bills to ensure that no tariff item has been hiked during the six months period specified in the Tariff Order. ▪ To verify from bills of subscribers who have changed their tariff plans to ensure that no migration charges have been levied.
1.2	The information required in the clause above shall be available on the Service Provider's web site, as prescribed in TRAI Direction No.301-26//2003-TRAI (Econ.) dated 2nd May, 2005 (Format- C).	▪ Obtain website URL. ▪ Log onto website and verify whether mentioned details are available for each Tariff plan. ▪ Establish whether above information is available on the website in accordance with TRAI directives.
1.3	Where a value-added service (e.g. download of content, such as a film clip or ring tone) or entry to an interactive service (such as a game) can be selected through a choice of the service user	Take a list of all value-added services. Take sample from each value-added service and check the procedures completely.

Sr. No	Audit Area (item name)	Test to be performed
	(e.g. by dialing a specific number) then the charge for the service must be provided to him before he commits to use the service.	Verify whether the charge for the service is indicated before subscriber commits to use the service.
2	**Provision of Service**	
	The services provided to the customer and all subsequent changes therein shall be those agreed with him in writing prior to providing the service or changing its provisions.	▪ Verify procedures to log customer requests for services. ▪ Verify procedures for applying such customer requests.
3	**Accuracy of Measurement**	
3.1	All charges must be consistent with the published Tariff applicable to the end-user charged.	▪ Verify with 3 months CDRs with reference to tariff plan opted by customers and by making calls in each selected plan
3.2	a) Unless otherwise specified in the published Tariff or previously agreed Tariff, a charge shall be determined in accordance with the following limits: b) Where the charge is dependent upon duration, the recorded duration shall be measured to within: ▪ Between +1 seconds and –1 second; or ▪ Between +0.01% (1:10,000) to –0.02% (1:5,000) whichever is less stringent; and	▪ Test check sample records to establish correctness of parameters.
	b) where the charge is dependent upon the time of day, the time of day shall be recorded to within ±1 second, traceable to an appropriate time reference; and	▪ Test check sample records to establish correctness of parameters.
	c) where the charges are dependent upon the counting of occurrences of a particular type, the count shall be accurate to no more than plus 1/25,000 (0.004%) or minus 1/1,000 (0.1%).	▪ Test check sample records to establish correctness of parameters.

<table>
<tr><th>Sr. No</th><th>Audit Area (item name)</th><th>Test to be performed</th></tr>
<tr><td>3.3</td><td>Where measurement under clauses 3.2 (a), (b) & (c) reveals systematic errors in timing or counting that result in overcharged events which are not stated in published Tariffs then correction should take place to ensure accurate Bills.</td><td>▪ Verify with the records whether corrective action has been taken.</td></tr>
<tr><td>4</td><td>Reliability of Billing</td><td></td></tr>
<tr><td>4.1</td><td>The performance of a Total Metering and Billing System shall be, subject to the tolerances specified in clause 3.2:
a) the numbers of items of service usage that are overcharged events or undercharged events, as a proportion of the total number of chargeable events, shall not exceed the limits shown in Table 1; and

b) the sum of the values of the errors in the overcharged events or undercharged events, as a proportion of the total value of the total number of Chargeable events, shall not exceed the limits shown in Table 1.

Table 1 – Total Metering and Billing System reliability performance requirements
<table>
<tr><td>Chargeable Events</td><td>Performance</td></tr>
<tr><td>Number under or not Charged</td><td>0.1% (1 in 1000)</td></tr>
<tr><td>Number overcharged</td><td>0.004% (1 in 25,000)</td></tr>
<tr><td>Value under or not charged</td><td>0.05% (1 in 2000)</td></tr>
</table></td><td>Based on the audit procedures applied above, take the total deviation and verify whether the same is in accordance with the limits stated by TRAI</td></tr>
</table>

Sr. No	Audit Area (item name)	Test to be performed
	Value overcharged | 0.002% (1 in 50,000)	
4.2	Where implementation of an order for a service, feature or discount which depends on the number or duration of chargeable events is applied at variance with published Tariffs, each chargeable event within the scope of the incorrectly applied order shall be an undercharged event or an overcharged event, as appropriate, for the purposes of clause 4.1.	Verify with reference to tariff plan
4.3	Where an item of service usage is completed other than intended, but the charge applied is correct for the service as delivered, this shall not be regarded as either an undercharged event or an overcharged event.	Observation
4.4	The increase in duration or number of items of service usage resulting from degraded transmission performance shall not be taken into account when computing the performance of the system.	Observation
5	**Applying Credit to Accounts**	
5.1	**For post-pay accounts**, payments made by a customer shall be credited to his account within 3 working days of receipt of the cash/ cheque. Where credit is given by the service provider, this shall be applied within one working day of its agreement.	▪ Review the payment credit system. ▪ Take payments sample to check whether the credit is applied correctly. ▪ Check that the payments made by the customer are regularly updated in the billing system. ▪ Updation in respect of post-pay customers to be credited within 3

Sr. No	Audit Area (item name)	Test to be performed
		working days of receipt of the cash/cheque.
5.2	**For pre-pay accounts,** top-up credit shall be applied to a customer's account within 15 minutes of its application. Where credit is given by the service provider, this shall be applied within 1 day of its agreement.	▪ Review the system settings and take sample cases to test whether the conditions are met.
6	**Timeliness of Post Pay Billing**	
6.1	The timeliness of bill issue or bill data file issue shall be subject to systematic processes.	▪ Review process and procedures for issuance of bill.
6.2	Any chargeable events the details of which are not available when the bill is prepared shall be included in a subsequent bill, but not later than the fourth monthly bill after the chargeable events occurred. Any details not so presented shall be written off and if significant be counted against the performance for undercharged events in clause 4.1. Exceptionally, event details from a separate service provider may be billed up to three months after receipt.	▪ Review the process of chargeable events. ▪ Take sample for such cases (typically where the customers are National or International Roaming). ▪ Obtain list of all such events (that have occurred) for the period under review. ▪ Review procedures of inclusion of such events in subsequent bill (Whether such charges are separately identifiable). ▪ Review procedures for writing off of such charges. ▪ Verify whether all such charges have been included for calculation of 'undercharged events' ▪ Check that all calls billed are in respect of the billing period referred on the bill and also to verify whether the discounts, if any, have been properly passed on to the customers without any errors.

Sr. No	Audit Area (item name)	Test to be performed
6.3	Agreement to extend the timescales described in clause 6.2 may be sought from the TRAI. An extension will only be available on an irregular basis. Decisions will be made on application for an extension concerning: **a)** The method in which how customers will be informed of a protracted delay in rendering call records onto a subsequent bill; and **b)** The integrity of the billing process audit arrangements.	▪ Review any exceptions sought from TRAI for extension. ▪ Review the method in which such clients have been intimated and verify the process for such issues ▪ Verify whether there is appropriate audit procedures implemented within the company to address such issues
6.4	The service provider shall contract with its delivery agent to ensure that an effectual bill or bill data file delivery schedule is in place. The existence of such a contract shall be subject to audit.	▪ Obtain & verify all bill delivery vendor contracts ▪ Test & establish effectiveness and adequacy of procedures and process
7	**Restriction and Removal of Service**	
	Where the service provider unilaterally intends to restrict or cease service to the customer, a notice shall be provided to the customer in advance of such action so that the customer has reasonable time to take preventive action to avoid restriction or cessation of service.	▪ Understand related procedures and establish adequacy thereof ▪ Test similar instances during review period and establish adherence ▪ Check that proper notices are sent to the customer in advance where the service provider unilaterally intends to restrict or cease service to a customer.

Sr. No	Audit Area (item name)	Test to be performed
		▪ In case of disconnection due to payment made beyond credit period, to check that the services get restored once the payments are made within the period as stipulated by TRAI.
8	**Complaint Handling**	
8.1 8.2 8.3 8.4	The service provider shall have a documented process for identifying, investigating and dealing with billing complaints and creating appropriate records thereof. The service provider shall carry out a root cause analysis for each upheld billing complaint, categorise the cause and establish proportionate remedial action to correct it. Where the root cause affects multiple customer accounts, then all affected Bills shall, if practicable, be included in a recovery programme. Where remedial action has not been completed and the cause is likely to affect other bills when issued, then the service provider shall take reasonable steps to ensure that they are checked and, if necessary, corrected, before being sent to the customer. If not checked and corrected such Bills shall be included in a recovery programme.	▪ Check whether the service provider has a documented process for identifying, investigating and dealing with billing complaints. ▪ Review the Billing Complaint system ▪ Review process manual for addressing customer complaints and establish adequacy of procedures ▪ Test instances during review period and establish adherence to documented procedures ▪ Review & verify procedures for root cause categorization and analyses ▪ Check whether the service provider carries out root cause analysis for each upheld billing complaint and where the root cause affects multiple customers, whether all affected bills is included in a recovery program. ▪ Test and verify instances of remedial action ▪ Verify adequacy of procedures in this regard ▪ Check the true and correct position about specific instance of billing complaints having systemic/ generic implications as referred by TRAI.

Sr. No	Audit Area (item name)	Test to be performed
9	**Materiality**	
	Compliance with the requirements contained in this regulation shall need to be demonstrated only in relation to products and services that have a material impact on the customer's bill. This materiality is deemed to be: a) where the service provider's turnover from a product or service comprises 5% or more of its total turnover with the customers targeted for that product or service; or b) where the number of customers subscribing to a product or service offered by the service provider comprises 5% or more of the customers targeted for that product or service; or c) at the specific direction of the TRAI.	Observations, if any
10	**Submission of Compliance**	
	The service providers shall submit the compliance of above code of practice to TRAI on yearly basis.	

Billing & Metering System Review (Transaction Review)

Sr. No.	Audit Area (item name)	Test to be performed
1	The auditing Agency shall evaluate inter alia the correctness of the following: - (a) In generation process of the CDR-raw CDRs.	▪ Test check procedures for CDR recording for both pre-paid and post-paid plans ▪ Verify whether CDR's are editable
	(b) Of the entries in the direction table	▪ Verify rating masters to establish

	which is used for rating the raw CDRs.	procedures for creating and modification of service charges ▪ To verify the proper configuration of all the tariff plans in billing system. ▪ Verify rating masters to establish charges mapped to each tariff plan ▪ Test whether rated CDR's are modifiable.
	(c) In charging of VAS services to the subscribers.	▪ Obtain list of all VAS services ▪ Verify procedures for mapping of charges to VAS services ▪ Verify whether any VAS provided without consumer's consent and charged. ▪ In respect of services provided during "Free Trial Period" to subsequently check whether the customer has confirmed the continuance of services once the free trial period has ended and accordingly billed for.
	(d) Of the rated CDR vis-à-vis the rated applied, duration mentioned, origination and destination codes including STD/ISD destinations, both for mobile and fixed.	▪ Verify procedures for mapping of call origination and destination locations. ▪ Raw CDR's to be rated according to the Tariff Plans and Rating Algorithms (set of tables/ rate masters) ▪ Check all billable activities occurring on the network are accurately captured, rated and billed in accordance with customer agreement. ▪ Check that there is no delay in updation of billing with latest agreed upon rates/ tariff implementation. ▪ Due to non-updation / rating, a CDR generated may go to suspended CDR's pool which may be billed subsequently. In such cases to check that it is billed subsequently for the same period and is in line with the agreed Tariff Plans. ▪ To check discounts / schemes not forming

		part of the original contract are properly passed on by the Service Providers in respect of the various marketing schemes promoted by the Service Provider from time to time.
	(e) In charging of the roaming services to the mobile subscribers	▪ Verify procedures for applying roaming charges and also evaluate inter alia the correctness as per the published tariff.
2	The Audit Agency will take the raw CDRs & process the same to generate the Bill and then verify with already generated bill for any discrepancy. The CDRs of last three months are to be processed.	▪ Obtain CDR's for selected audit sample ▪ Apply procedures on selected sample ▪ Compare the results to ensure that the service provider systems are functionally correct.
3	The Audit Agency will analyse the discrepancy if detected, and find out the root cause of the same. Discrepancy Analysis The discrepancy analysis is done by execution of the inference engine that performs analysis of the rated CDRs in order to establish causes of the discrepancy based on CDR, subscriber and pricing plan data.	Discrepancy analysis of the rated CDR's to be done. If required perform further functional testing on system to identify the cause
4	Bill level discrepancy analysis. After several cycles of event level discrepancy analysis and database adjustment, when all the event level discrepancies are taken care of, the next step is of bill level discrepancy. The bill level discrepancy reports will be produced & analysed by the audit Agency.	To analyze the bill level discrepancy reports as generated by the Service Provider.
5	Verification of corrective actions. In this important stage, a verification of	Analyse and tests check the corrective actions.

	successful implementation of the corrective action is performed	
6	Billing system integration for rental rebates (for basic service). (Reference – Regulation on Quality of Service of Basic and Cellular Mobile Telephone Services, 2005 dated 1st July, 2005)	Verify that the billing system is integrated so as to ensure that proper rental rebates are passed on to the customer in cases where the faults are not rectified within three days (for basic service). • Faults pending for >3 days and <7 days: Rent rebate for 7 days. • Faults pending for >7 days and <15 days: Rent rebate for 15 days • Faults pending for >15 days: rent rebate for 1 month

****

Chapter 20
Audit of Functional Areas

Every organisation would have Standard Operating Procedures (SOP) to ensure internal control and proper functioning of these departments. Hence, it forms the main basis for the internal auditor to evaluate these functions. The internal auditor should ask for the copies of all the SOPs used by an organisation. In case, there are no written down SOPs in vogue, the internal auditor should discuss with the management/heads of departments and then document these for each department. The internal auditor has to refer to the overall operating framework of policies, practices, systems, management philosophy, values and actions which exist in an organization to ensure that:

- essential organization objectives are met;
- assets are protected and risks are managed;
- legal requirements are met;
- information used to report to Revenue is accurate.
- Compliance with the internal control procedures & risks asserted
- The incidences of wastages & misappropriation
- The expenses incurred during a period and the trend of expenses over a period of time
- Operational efficiencies of the departments

The general procedure to be followed for internal audit of the support departments is suggested as follows:

- Setting of the internal audit objectives with regard to the audit criteria/benchmark so that the causes for the variations could be assessed and reported along with the effect of such variations on the organization.
- Setting the scope of the audit with regard to the audit period, the audit units such as locations/ departments etc. so that the resources could be planned.
- Collect the information on the departmental activity carried out, the budgets etc. from various sources of information.
- Put forward the results of internal control review through control testing procedures carried out.
- Summarise the report for the department.

Review of Internal Control

Management has the responsibility to devise and maintain an adequate system of internal control for its operations. Internal controls are the overall means whereby management ensures that objectives are met, risks are assessed and managed, appropriate reviews of the operation's performance are made, and

that information sharing and communications occur in a timely, accurate and appropriate fashion, with due regard for protection of valuable information.

However, to judge its effectiveness it is necessary that internal auditor should ask the following questions:

- Does the company have a functioning Audit Committee.
- Is the audit made on a surprise basis rather than scheduled in advance.
- Is an audit also performed when there is a change of officers.
- Are records of the audit documented and the results kept in the files.
- Controls on the financial information dissemination

Administration Department

The significance of an administration department assumes a different proportion in the Telecom industry. In many companies administration department may be combined with HR or accounts depending upon the size of the organisation. The checklist given below is based on the assumption of a separate Administration department:

- Define the audit objective and scope of the work
- For each administrative process, study the SOPs, schedule of authorities etc.
- Decide the sample size and obtain sample data as an audit evidence
- Observe the variations with respect to the SOPs
- Assess the risks and value impact on the organisation
- Arrive at the audit findings and conclusions
- Areas to be checked in administration:
  - Office routine procedures for authorisation and approval
  - Office maintenance and utilities
  - Compliances with laws such as Shop act, Weights & measures, property tax laws etc.
  - Office rental agreements and compliance
  - Health, safety and environmental aspects
  - Factory administration compliances such as Factory Act, Payment of wages act, Minimum wages act etc.
  - Administrative purchases and policies thereof
  - The total administrative expenses analysis v/s budgets
  - Administration expenses as a percentage of total cost of sales and the trend over a period of time

MIS generated periodically on the administrative matters

Procurement Department:

In the Telecom industries the procurement may not actually involve buying of raw material, but may be

required to buy utilities and services. In light of this the internal auditor should analyze the operating activities of procurement department. The following general checklist may be suitably amended to suit the needs of Telecom industries:

- Obtain the purchase procedures regarding vendor sourcing, vendor registration, vendor evaluation, quotation, tendering, vendor selection, and ordering
- Assess how the procurement quantity and time of requirement decided through the indenting process
- Assess how the ad-hoc and emergency purchases handled
- Are the POs issued as per the schedule of authority.
- Receipt of materials to be only against valid purchase order and from registered vendors
- Process of material acceptance with regard to the specified quality norms
- Appropriate insurance coverage for the inventory
- Physical stock taking procedures and reconciliations with the book records
- The contracts with vendors (long terms & short term), rate agreements, quantity agreements
- The documents for verification:
    - Requests for proposals (RFP)
    - Quotation/tender analysis sheets
    - Purchase orders
    - Inventory verification & reconciliation sheets
    - Financial and cost accounting records

Finance and Accounts department

The focus of the internal auditor should be on compliance with the accounting standards as may be applicable, but keeping in view the peculiar activities of the Telecom sector. The internal auditor should take into account these specific aspects of accounting.

The checklist for the accounts and finance departments would be as follows:

Accounting

- The accounting policy adopted for treatment of different financial elements such as incomes, expenses, assets, liabilities and equity
- The accounting system used such as ERP
- The chart of accounts, master accounting data and automated accounting entries for accounting of financial and non-financial transactions
- The appropriateness of the accounting policies to be consistent with the accounting standards
- The integrity of the accounting system e.g. completeness of the double entry principle in correctly updating the relevant tables in the database

- The controls of the various ledgers such as AR. AP, GL, fixed assets, etc.
- Authorisation and approval processes for accounting entries like journal entries, adjustment entries and rectification entries
- Access control to the accounting system to avoid unauthorized entries
- Accounting reconciliation statements such as bank reconciliation, AR & AP reconciliation
- Physical verification of cash, bank balances, fixed assets etc.
- Appropriate insurance covers of cash and fixed assets
- Identification of non-performing assets
- The trial balance reports and integrity checking on a continuous basis
- The data on disclosures required in the financial statements

  The documents for verification:

  - Expenses vouchers
  - Journal vouchers
  - Invoices – sales and purchases
  - Debit and credit notes
  - Bank statements for current a/c & other balances
  - FD receipts
  - Cash receipt & payments book
  - Cheque books, cancelled cheques, e-cheques
  - Electronic banking accesses and controls of authority, the electronic dongles & their custody
  - The ledgers and fixed assets registers

Finance

- The policies and procedures adopted for financial management processes
- The schedule of authority included authorized signatories for banking and such other transactions
- The policy on capital structure
- The methods of raising funds, the authorities for raising loans etc.
- Loan document registration and filing
- Interest payments and maintaining the loan agreement covenants
- The trends in financing costs
- The methods of capital expenditure evaluation
- The debt ratios, interest cover ratios
- The banking facilities and agreements for consortium or independent banking
- The authorisations for banking transactions
- The data utilisation (and non-utilisation) of bank facilities

Receipt of Revenue:

General principles of revenue recognition as per AS 9 are to be applied, the revenue recognition aspects in the telecom industry are different. In a telecom company revenue is generated from Billing to Post Paid Subscribers, Billing to Broadband Customers, Billing to IDC Customers, Sales of RCV's / E-recharge and Sales of Handsets and Accessories etc. The Internal Auditor has to determine that proper procedures are followed in handling of receipt from customers and review the records to determine whether the required reports are being accurately and promptly prepared.

- Verify proper booking of all the receipts and amount received is correctly accounted in the customer's account.
- Are receipts of cash and remittances posted accurately and on a daily basis in the correct account
- Amount received promptly deposited in an interest-bearing account.
- Are funds that have not yet been deposited adequately protected.
- Delay in depositing/ non-depositing the amount collected in the bank.
- Verify proper safeguards of accounts, signatories on bank accounts and verify that all Bank Accounts are in name of company.
- Verify the process of reconciliation of various bank accounts and controls in place to ensure collections made at various collection centers are properly monitored.
- Management of bouncing of cheques of customer.
- Delay in transfer of amount collected to central pool account.
- Proper control over printing, issue, use of Manual Receipt Books and reconciliation of used receipt books.
- Are the Receipts Journal and Disbursements Journal summarized on a monthly basis.

Expenditures: Review and Approval

- Verify that all significant expenditures are properly recorded
- Verify proper voucher approval procedures.
  a) Determine if routine expenses receive less than full scrutiny and approval
  b) Test a sample of expenditures, especially those to individuals
- verify proper approval obtained for expenditures
- test for reasonableness of expenditures
- verify that goods or services were received
- Bills presented for payment should be reviewed and the following verified:

- Are bills made out to the individuals or to the company. Are those bills legitimate expenses and are they dated.
- What controls are in effect to prevent duplicate payments.
- Are discounts taken where appropriate.
- Is the arithmetic on the bill correct.
- If corrections are made to a bill, are the incorrect figures ruled out (not erased or obliterated) and the corrections signed by the person approving the bill.
- Are all bills certified correct by the person who knows that the expenses are authentic.
- Are all bills properly approved by the appropriate designee.
- Are all paid bills, statements and expense vouchers kept for records.
- Does each bill and expense voucher paid show the check number, payment date, to whom paid, and the correct account classification code for the expense.
- Are any individuals approving their own expenses.

Disbursements

Money from bank accounts used during ordinary business activities are to be spent only on the basis of approved bills and expense vouchers. Internal Auditor should review the following:

- Is the money withdrawn from Bank account used strictly for the purpose it is withdrawn.
- Have any cheques or withdrawal slips been signed by the same officer who approved the expenditure or withdrawal.
- Are all Banks accounts reconciled with the bank statements promptly each month.
- What is the procedure if discrepancies in the reconciliation are uncovered or if there are unusual or suspicious circumstances about disbursements or authorization for payment.
- The auditor should reconcile the bank accounts on a random basis during the audit.

Advances

Internal auditor should review the advance paid to staff/ third parties. Outstanding advances should be reviewed as follows:

- Are advances to staff / third parties approved by the appropriate authority.
- Are such advances made for periods normally not exceeding the period as per company policy.

Records Retention

Internal auditor has to verify that the company keeps records that support items reported on their books or tax returns until the statute of limitations for the return expires. The internal auditor must determine that certain legal requirements are being met, including:

- Were any licenses or permits required for an activity duly obtained.
- If special taxes (property taxes, Service tax, excise taxes, VAT etc.) were due, were provisions made to remit them?
- Determine and verify applicable use of state Sale Tax/VAT tax reporting.
- If service tax are collected and deposited in time.
- Verify that all offices are reporting on a regular basis and that their data is included in annual Telecom Annual Reports.

Human resources and Personnel department

The general function of the HRD is to decide and implement policies and procedures with regard to the manpower resource of an organisation. Telecom Industry depends heavily on its manpower. The staff may be appointed on permanent or contract basis depending upon the need. Hence, the internal auditor should carry out the audit of this department taking into account the specific objectives thereof. The following general checklist may be used with suitable adjustments as may be necessary:

Control parameters to be checked:

- Standards for hiring employees specifying professional qualification, education, experience, and other skill sets.
- The process of recruitment followed e.g. through consultants, campus recruiting etc.
- The candidate screening procedures such as interviews, tests, reference check, medical checks etc.
- Training & induction rules.
- Policy on performance evaluation and salary increase, incentive schemes.
- Rules for disciplinary actions.
- Assigning responsibilities and job profiling.
- Empowerment of the staff.
- The whistle blowing policy.
- The policy & procedures about code of conduct, ethics and other organisation values
- Verify the impact of contingencies related to the labour court cases.
- Verify the cases of misappropriation & fraud by the employees.

Salary audit:

- Check if the appointment letter are properly authorized and are as per the policies
- Assess the overrides in the salary agreed which is different than the normal scales
- Obtain information on the incentive plan for individuals & groups at all the levels of

management

- Understand the parameters for incentive calculations and compare the actuals with the plans
- Verify the incentives approved with regard to the measured performance
- Check the incentive calculations to verify the correctness
- Verify the monthly payroll processing procedure, whether in-house or outsourced
- Verify the deductions and check the correctness thereof e.g. taxes & applicable TDS rules
- Check the disbursement procedures to verify the correctness of the ECS to the individual bank accounts
- Check the reconciliation of the salary sheets with the previous month to verify the reasons for the change such as new employees added, employees left, salary changes etc.
- Observe the payroll risk areas such as time keeping & time booking, salary changes, etc.
- Verify the master files of the employees with the payroll processed data
- Check the records for leave, absenteeism, etc.
- Verify the contributions to PF, superannuation, gratuity and such other benefits
- Obtain confirmations from the managers of the contributory plans to correctly determine the value of plan assets & plan obligations
- Obtain the information about the basic assumptions made for the actuarial valuation of the benefit obligations
- Verify the schemes of ESOP for allotment of shares
- Verify that employees left do not appear in the payroll
- Check the cases of full & final settlement for accuracy of calculations
- Verify the accounting entries for the payroll for the period
- Is the company complying all the labour laws and other statutory laws being a principal employer in case manpower employed through outsourced agency.
- Verification of employees actually employed for work through outsourced.
- The attendance, leave records and payroll processing of manpower providing agencies.
- The internal auditor should verify that the company has proper systems and processes to control integrity and security of data handled by contractual manpower these aspects.

Performance ratios

- Percentage of staff cost to total cost
- Revenue per employee or revenue per rupee of salary cost
- Labour turnover ratios
- Incentive rewards as percentage of salary costs
- Idle time percentages & its impact on the costs

Sales and Marketing

Telecom companies are incurring huge expenditure on sales, distribution, marketing and publicity due to fierce competition and high business growth in the industry. The telecom companies are providing various incentive scheme, commissions to the dealers and channel partners to motivate them to acquire more business for the company and they also incurring huge marketing expenses and providing attractive sales schemes to attract new customers and retain their old customers. The following general framework would help the task of the internal auditor:

Control testing on segregation of duties:

- Credit decisions
- Billing
- Dispatch
- Collection of dues
- MIS on sales & marketing Accounting
- Pricing policy and discounts
- Competitors' prices
- Credit policy of the company including credit terms, credit limit and credit period
- Distribution network
- Credit assessment of customers
- Credit evaluation norms
- Customer payment history trends
- Bad and doubtful debts
- The sales orders information
- Sales data customer-wise, location-wise, product-wise
- Understanding of total market size, market share of the company
- Brand image and value
- Sales performance v/s plans
- Policy on appointment of dealers, Channel Partner's
- The Channel Partner's expenses such as customer acquisition commission, sales incentives, and collection commission are properly accounted.
- verify the existence and efficacy of the database for making various payments to channel partners.
- Verify that sales are not inflated by the dealers/ distributors to achieve the targets.
- verify the methods and process to monitor promotional schemes expenses.
- Verify the system and process of identifying the eligible winner for prizes of promotional schemes.

- Marketing expenses such as advertising, promotion, incentives, commissions etc.
- Advertisement through Print media, Hoardings, Signage, Electronic Media, Sponsorship of events.
- verify that advertisement is displayed at the contracted location,
- Verify that advertisements on hoardings are displayed at various location sites for a contracted period.
- Verify the provision for change of advertisement contents during the agreement period.
- In the case of radio and TV advertisements, ensure that Broadcast/ display of advertisement for agreed time slot.
- Verify that advertising agency has passed on all the discounts on rate negotiation to the company in case of bulk advertising.
- Verify that telecom company has a proper understanding with the shopkeeper about return of Signages.

Performance indicators for sales & marketing such as

- New customers added
- Customer drop out ratio
- Customer complaints & their resolution
- Increase in market share
- Customer satisfaction index

The IT Department

Telecom industries is highly IT enabled sector. Telecommunication companies invariable get access to the IT system to do their transactions which are then directly linked to the database of the IT system. The IT department within the organisation has to perform duties to ensure that the systems are absolutely safe, user-friendly and available all the time. The job of an internal audit essentially becomes important to check strict adherence to internal controls, risks related to the safety of individual accountholder's information, probabilities of unauthorized access, possibility of hacking etc.

It naturally becomes a potentially vulnerable area for audit. The internal auditor should exercise utmost care and diligence in carrying out the audit procedures that are related to the IT systems in the service organisation as mentioned above.

The *control parameters* that the internal auditor should concentrate on could be:

- The IT management including access control, back-up and recovery, IT environment costs
- IT inventory
- IT operations
- IT security related to the system design

- IT service agreements
- Data protection e.g. antivirus, antimalware, internet related securities

The following checklist would help the internal auditor to conduct the audit of the above named control parameters of the IT department

IT department structure

- Whether the function is fully in house or outsourced or a combination thereof
- Checking of the service agreements for outsourced IT services
- The profile of the IT personnel (professional as well as others)
- Reporting of the IT department
- Are the IT staff allowed to input transactions in the system (this is a potential risk)

IT inventory

- The physical verification of the IT inventory (hardware, operating system software, networking equipment and application software etc.) at all locations
- The maintenance contracts for the IT equipment
- Equipment replacement policy
- Equipment and software license status

IT processes

- Are the IT processes clearly defined in the manual?
- Is there a proper documentation regarding system design, application programs, database administration, data entry, disaster recovery & back up processes?
- Checking of the processes for making changes to the programs, authorisation thereof, testing procedures
- Test checking of documentation

Access control audit

- Who have the access to the system documentation?
- Is there any access trail available?
- What is the access control to the system & application software?
- What is the control on the data files?
- Who can access the on-line system?
- What is the password administration procedure?
- Is the access blocked on a number of failed log-In attempts?

- Controls related to generation and circulation of reports through email and other communication methods

Risks assessment

- Risks arising and their impact on the organisation and those external people who access the system
- Risks of unauthorized changes to the hardware and software
- Risks related to authorized log-in and system abuse
- Risk arising out of system failure
- Risks arising from loss of system integrity

Risks arising from virus to the system program and the application software

The internal auditor should test the above areas by:

- Checking the documentation for its completeness
- Sample checking the access controls, password controls, virus controls
- Analytical procedures to verify the instances of variation

Billing and Customer Care System

The Billing and Customer Care System (B&CCS) is an integrated customer care, billing and accounting platform and supports flexible billing for wide range of Telecom services, viz. Tele-services, Bearer services, Supplementary services, GPRS, WAP and IN services etc. It is primarily responsible for activation, deactivation suspension of subscribers, provisioning /de-provisioning of various services to the subscribers and billing for the various services used by the subscribers.

The major functions of B&CCS are

1. Inventory and SIM management.
2. Activation/deactivation of mobile numbers.
3. Provisioning / de-provisioning of various services to the subscribers.
4. Handling of requests from customer care centers regarding telephony services and billing queries.
5. Swapping of SIM and MSISDN.
6. Collecting, processing and storing of CDRs (Call Detail Records) from the Network elements.
7. Rating the CDRs and Billing.
8. Payment and Collection
9. Billing for Inter connect Usage Charges
10. Provision for testing new products / services before commercial launching.
11. Threshold monitoring.
12. Intrusion detection and Fire wall functions.

13. Trouble Ticket (Remedy) system.
14. Handling of TAPIN & TAPOUT for Revenue settlement with roaming partners.

Bill Verification

Internal auditor has to verify the following:

- Verify bulk and incremental discounts and tax at ion methodologies.
- BIP discount prorating when change in discount rate during bill cycle.
- Verify special balance-due amounts to exclude
    - Disputed amounts
    - Amounts in collections
    - Amounts on invoices whose payment date has not yet been passed
- Check different discount Rates & special rates based on customer category
- Verify special rate, discount or both with customizable plan Id
- Verify special rate, discount or both - Demonstrate Cross product discount
- Check Friends &Family using Corridor plan feature
- Verify invoice cycle including annual, monthly, bi-monthly, quarterly, weekly and even daily cycles.
- Various options with regard to the timing within each bill cycle when the customer receives an invoice
- Verify Invoice timing enabling customers to change invoice cycles.
- Verification of Discount based on the accumulated gross amount of qualifying usage charges during a specified period Discount should get applied only on usage that falls between bill period
- Flexible formatting of Invoices Bill message flexibility should be there
- Preparation of detailed bill based on type of usage like Local, STD, ISD
- Separate taxes to both products and services
- Verification of tax in a flexible manner, either in the form of a fixed amount, a percentage or combination of both
- Display of Tax in flexible manner i.e. different components like education cess, higher education cess should be displayed separately and accordingly reports should be generated

Tests on Payments and adjustments:

- Check whether CSR is able to capture payment information using payment entry interface. The system should support Bar-Code reader Payment should be successfully applied

- Verifying support for cash, cheque and credit card payment entries
- Verifying support for ECS, Credit Card payment entries
- Check of miscellaneous credit adjustment, reversal of an adjustment against an invoice.
- Adjustment with and without service tax
- Check of daily account reconciliation both cash and all instruments.

Tests on Collection Process:

- Check for calculating outstanding debt for customers for call charges as well as non-usage charges, *as* per account category
- Check for reports with the list of customers exceeding their limit during Credit Limit Check
- Account category wise collection scenario
- Remove account from collection processes. After receipt of payment Assertive cure.
- Check write off module without outstanding limit
- Auto reconnection should happen taking into Account balance.
- Check for Circle wise collection reconciliation

Tests on Roaming:

- Check the agreement of partnership between local operator and remote operator
- Application of rate, tax& surcharge for in-roamer usage records
- Check Roaming system supports different rates for different operators and various reports as prescribed by Corporate office or for operational requirement

Revenue Generation related Reports:

- List of refunds effected
- Summary of New Mobile activated
- Monthly summary of refunds made
- Plan wise Revenue
- Monthly list of bills cancelled/ written off
- Check the operator wise list for TAPIN& TAPOUT call charges from/to other operators
- Check Roaming subscription charge report for National& international roaming

- CSR wise adjustments posted for each circle
- Check prepayments of past excess payments that are being adjusted in the current invoice, payment reversals for pre-payment and deposit payments
- Details of the cheque payment received containing cheque No., date of issue, bank details and the amount for a particular account number, cheque dishonor
- Check the heavy callers, low callers, customers with ISD facility

Ledger and Sub-ledger related reports

- Ledger review in respect of cellular phones
- Details of disconnection/reconnection/ closure
- Details of discounts and commission
- Details of aging outstanding details
- Details of unadjusted credits
- Details of surcharge
- Details of service tax
- Reports for customer statistics
- Reports for fault booking statistics

Chapter 21
Maintenance of Cost Records and Cost Audit

Applicability for maintenance of Cost Records under Notification of Ministry of Corporate Affairs

Telecommunication Company falls under the purview of maintenance of cost records as per following notification.

(Extract from the Notification of Ministry of Corporate Affairs (MCA) Notification 7th Dec. 2011)

"G.S.R. 869 (E). - In exercise of the powers conferred by sub-section (1) of section 642, read With clause (d) of sub-section (1) of section 209 of the Companies Act, 1956 (1 of 1956), and In super session of the Cost Accounting Records (Telecommunications) Rules, 2002 vide G.S.R. 689(E), dated the 8th October,2002, except as respects things done or omitted to be done before such supersession, the Central Government hereby makes the following rules, Namely Cost Accounting Records (Telecommunication Industry) Rules, 2011: -

(1) The following services or activities provided by the company, including such services that require license or registration with the Ministry of Communications and Information Technology, Government of India, namely: -

(i) Basic Telephone Services;
(ii) National Long Distance Services;
(iii) International Long Distance Services;
(iv) Cellular Mobile Telephone Services;
(v) Wireless Local Loop (WLL) (Fixed or Mobile) Telephone Services;
(vi) Very Small Aperture Terminal Services;7
(vii) Public Mobile Radio Trunk Services;
(viii) Global Mobile Personal Communication Services;
(ix) Internet or Broadband or Wireless Access service;
(x) Infrastructure Provider (IP-1);
(xi) Passive Telecom Infrastructure including Telecom Tower Facilities;
(xii) Cable Landing Stations; and
(xiii) Any other related, allied, intermediate or support services in relation to telecommunication activities not indicated above. National Long Distance Services

2. **Application, –** These rules shall apply to every company, including a foreign company as defined under

section 591 of the Act, which is engaged in the production, processing, manufacturing or rendering of telecommunication activities and wherein, the aggregate value of net worth as on the last date of the immediately preceding financial year exceeds five crore of rupees; or wherein the aggregate value of the turnover made by the company from sale or supply of all products or activities during the immediately preceding financial year exceeds twenty crore of rupees; or wherein the company's Equity or debt securities are listed or are in the process of listing on any stock exchange, whether in India or outside India:

Provided that these rules shall not apply to a body corporate which is governed by any Special Act.

3. **Maintenance of records, –**

(1) Every company to which these rules apply, including all units and branches thereof shall, in respect of each of its financial year commencing on or after the date of this notification, keep cost records and the books of account so maintained shall contain, inter-alia, the particulars specified in Proforma A to H, mentioned below:

Proforma	**Particulars**
A	Service-wise Costing Profit and Loss Statement
B	Product or Network Service-wise Costing Profit & Loss Statement
C	Cost Sheet - Network Elements
D1	Apportionment of Support Functions to various Services (For PROFORMA 'D2')
D2	Apportionment of Support Functions to various Products (For PROFORMA 'B')
E	Statement of Capital Employed
F	Statement of Allocation or Apportionment of Capital Employed to Products or Network Services
G	Profit and Loss Reconciliation Statement
H	Capital Employed Reconciliation Statement

(2) The cost records referred to in sub-rule (1) shall be kept on regular basis in such manner so as to make it possible to calculate per unit cost of production or cost of operations, cost of sales and margin for each of its products and activities for every financial year on monthly or quarterly or half-yearly or annual basis.

(3) The cost records shall be maintained in accordance with the generally accepted cost accounting principles and cost accounting standards issued by the Institute; to the extent these are found to be relevant and applicable and the variations, if any, shall be clearly indicated and explained.

(4) All such cost records and cost statements, maintained under these rules shall be reconciled with the audited financial statements for the financial year specifically indicating expenses or incomes not considered in the cost records or statements so as to ensure accuracy and to reconcile the profit of all product groups with the overall profit of the company and the variations, if any, shall be clearly indicated."

Cost Audit

1. Applicability for Filing of Cost Audit Report

As per Notification dated 6th November, 2012 cost audit order issued by Cost Audit Branch of Ministry of Company Affairs, Government of India, Cost Audit report to be filed by including a foreign company as Defined under Section 591 of the Act every company is applicable to as follows :

a) the aggregate value of net worth as on the last date of the immediately preceding financial year exceeds five crores of rupees;
b) or wherein the aggregate value of the turnover made by the company from sale or supply of all products or activities during the immediately preceding financial year exceeds twenty crores of rupees;
c) or wherein the company's Equity or debt securities are listed or are in the process of listing on any stock exchange, whether in India or outside India.

2. Activity Groups for Telecommunication Services for Filing Cost Audit Report

The following activity Groups are prescribed by MCA for filing Cost Audit Report:

Sl.No.	Activity Group Code	Name of the Activity
1	5103	Internet and broadband services Not Applicable
2	5104	National long distance services Not Applicable
3	5105	International long distance services Not Applicable
4	5106	Public mobile radio trunk services Not Applicable
5	5107	Global mobile personal communication services
6	5108	Passive telecom infrastructure and tower facilities
7	5109	Cable landing stations Not Applicable
8	5121	Broadcasting and related services Not Applicable
9	5131	Performing art and entertainment services
10	5141	Other communication services not elsewhere specified

Cost Audit report includes 11 Annexure which is defined below:

Ann.	Particulars	Brief Description of Annexure
1	General Information	It includes general information like company name, CIN, E-Mail etc.
2	Cost Accounting Policies	Here we are required to report the policies adopted by company for the maintenance of cost records.
3	Product Group Detail	Here we are required to report revenue from different products which are covered under Cost Audit.
4	Quantitative information	Includes capacity details of equipment employed by the company for providing service.
5	Product Group Wise Abridged Cost Statement	It is a complete cost sheet which is prepared for each product group separately which is covered under Cost Audit.
6	Operating Ratio Analysis	It is Ratio analysis of different cost group with previous year.
7	Profit Reconciliation Statement With Financials	It is a kind of reconciliation between financial accounts and cost Accounts.
8	Value Addition Statement	Here we are required to report the value addition made by company during the reporting period.
9	Financial Position and Ratio Analysis	Here we report different types of ratios i.e. PBT to Capital Employed, PBT to Sales, Debt Equity Ratio etc.
10	Related Party Transaction	Here we are required to report all the transaction made by the company in relation to sale & purchase of services with its related party as per AS-18.
11	Reconciliation Of Indirect Taxes	This is a reconciliation statement of Indirect taxes paid by the company during the reporting period.

3. Approval from of Board of Directors.

a) Draft Cost Audit Report should be submitted to the Audit Committee of the Company and further adopted by the Board of Directors.

b) Cost Auditor(s) present(s) performance appraisal report to the management containing various kinds of analysis on the cost audit report. He also discusses and suggests his observations resulted while auditing the cost records of the company.

Submission of cost audit report:-

- It is to be submitted online in XBRL format to Ministry of Corporate Affairs.
- Company is required to file Cost Audit Report within 180 days from the close of financial year.

Checklist for Internal Audit for Cost Audit Report.

1. Whether the Cost Auditor is duly appointed as per rules and regulations prescribed by the law.
2. Checking of Statutory requirement for cost audit like 23C, 23D etc.
3. Audit Plan for Commencement and completion of Cost Audit Report.
4. Whether Cost Records provided to the Cost Audit in stipulated time by the law.
5. Date of handing over of Cost Records and other requirements as sought by the Cost Auditor.
6. Period in which Audit is completed as compared to planned period.
7. Date of approval of Audit Report by the Audit Committee and submission to the Board of Directors.
8. Observations and qualifications, if any, pointed out by the Auditor and their remedial actions for the next year.
9. Date of Filing Cost Audit Report in XBRL mode online with the Ministry of Corporate Affairs.
10. Keeping of documents, workings, final cost records, Cost Audit etc. for future reference.

****

Chapter 22
Checklist for Information Technology and Statutory & Regulatory Compliances

I. Checklist for Information Technology

Checklist for Information Technology				
S.No.	Priority	**Particulars**	**Risk Associated**	**Methodology**
		User		
1	**A**	To ensure that user list is updated on a regular basis and is reflective of the actual number of the employees in the unit.	Login IDs of ex-employees can be used for unauthorised access & performance of the system also deteriorates.	Matching the list of login ids provided by IT with list of number of employees on roll from HR.
2		For Open VMS system ensure that the System Administrator establish the usability of each UIC (Unique Identifying Code), deleting those not required and updating the UIC to user groups (the rights of the users are defined through a UIC).	Login IDs in excess of requirement can be used for unauthorised access & performance of the system also deteriorates.	Specific steps to as per Open VMS environment.
3	**A**	To ensure the users in IT do not share their root login and the root login	In case of any unauthorised changes accountability cannot be fixed & root is guessable	User ID should be as per the user name & be given system administrator rights. In case root login is essential then it should

Checklist for Information Technology				
S.No.	Priority	**Particulars**	**Risk Associated**	**Methodology**
		should not be used to do any maintenance activities.	which may leave the system open to unauthorised access.	not be given rights of remote login.
4	**B**	To ensure that individuals performing database administration are separately authenticated i.e. they should be given different user IDs.	In case of any unauthorised changes accountability cannot be fixed.	Review the IDs given to all the system administrators.
5	**A**	To ensure that default users, scripts & passwords are changed / deleted from the system.	Authorised access of systems through default ids etc.	Check if the default ids, passwords & scripts given in the software / hardware manual are deleted as per the latest security patches.
		Access Control		
6		Ensure that proper network zoning is done appropriately inside the network.	Unauthorised access to another person's data which may result in data theft, deletion or alteration.	Ensure that V LANs are created using appropriate switches.
7	**A**	Rights given to all the users should be reviewed periodically and ensured that supervisory / administrator rights are not given to general users.	The risk of unauthorised changes increases if the rights of the users are not based on their job roles.	Verification of the "User Access Matrix" provided by IT.

Checklist for Information Technology				
S.No.	Priority	**Particulars**	**Risk Associated**	**Methodology**
8	**B**	Ensure that a Password Management Policy is in place and adhered to, wherein minimum password length, locking of ID after a defined number of consecutive login failures, password expiration period, maintaining of password history for a specific interval are specified.	Unauthorised access to another person's data which may result in data theft, deletion or alteration.	Checking the Password Policy configured in the server.
9	**A**	To ensure that the Security Access Manager (SAM- which stores passwords for domain and local computer account) database is in an encrypted form to prevent unauthorized access.	Passwords stored without encryption can be easily retrieved & used for gaining unauthorised access to the database.	Auditing tool like Nessus, Real Secure etc. need to be used.
10	**C**	Ensure that the network database of other circles is not accessible to	Unauthorised access to database of other circles.	Ensure that access control list is applied to segregate these databases from other circles.

Checklist for Information Technology				
S.No.	Priority	**Particulars**	**Risk Associated**	**Methodology**
		each other.		
11	**A**	Internet access is totally restricted in the Call Center systems.	Unauthorised transfer of data to outside sources.	Access to proxy should be restricted & the users should be created on the proxy for people accessing internet.
12	**B**	To ensure that internet access to employees has been given on the approval of their HOD/CIO.	Unauthorised transfer of data to outside sources.	Checking of the Internet access form given by the user & approved by his HOD.
13	**A**	To ensure that all the PCs should have a power on and screen saver passwords as a measure of data security.	Security of data at a risk in case system is left unattended for a period of time.	Check whether power on & screen saver passwords are enabled on all the systems.
14	**A**	Internet leases line should be terminated on an isolated router.	Any other network component attached to the router would be vulnerable to external intrusions.	Auditing tools & physical check of the router.
15	**A**	All external parties connecting to the network should be isolated from the internal network through a firewall.	Network would be vulnerable to intrusions through external network.	Physical check & configuration of the firewall to check the zoning.

Checklist for Information Technology				
S.No.	Priority	**Particulars**	**Risk Associated**	**Methodology**
16	**B**	Hard disk sharing should be restricted & allowed only on a work group basis.	Data can be shared across the network in an unauthorised manner.	Use of auditing tools like Languard & check the domain policy.
		Asset Control		
17	**B**	To ensure that licenses have been obtained for all the software used in the unit in sufficient numbers. Generate list of software being used which are expired, demo license copies.	Legal proceeding can be initiated by the software vendor for illegal use of their products.	Software inventory list mapped with the available licenses.
18	**B**	To ensure that the PC control sheet / hardware inventory list is updated on a regular basis.	Weak / inadequate control over hardware.	Physical verification of the assets with the list.
19	**A**	To ensure that back up of data is taken on a daily basis / as per the backup policy of the unit.	Business Continuity at a risk.	Review of the back up files / logs.
20	**B**	Ensure that the backup should be kept in a fire proof	Safety of the backup of the data can be at risk without secure	Review of back up procedures.

Checklist for Information Technology				
S.No.	Priority	**Particulars**	**Risk Associated**	**Methodology**
		safe in an offsite location - preferably a bank locker.	offsite storage.	
21	**C**	Process of management of the Locker access should be well documented.	Safety of the backup of the data can be at risk without secure offsite storage.	Review of back up procedures.
22	**A**	To ensure that the floppy drive and CDROM drive is physically removed from the Call Center Desktops.	Unauthorised transfer of data to outside sources.	Check if the drives are physically not present in the machines.
23	**A**	Floppy drive is disabled on all Desktops.	Unauthorised transfer of data to outside sources.	Check if floppy drive is physically not present in the machines.
24	**A**	Ensure that the operating system & applications both on desktops & servers have the latest versions of service packs / patches installed.	Systems can have vulnerabilities which can be exploited by a hacker.	Run update on the system to see of the latest service pack has been installed.
25	**B**	Ensure that individuals do not store or use illegal code such as - MP3 files, Unlicensed Video clippings, Pornographic files	Copyright infringements & using office equipments for entertainment purposes.	Scanning of the user machines for files with the following extensions mp3, ra, mpeg, dat, jpg, jpeg, bmp, gif, avi, wav etc.

Checklist for Information Technology				
S.No.	Priority	**Particulars**	**Risk Associated**	**Methodology**
		and images, Copyrighted images and documents.		
26	**C**	Ensure that personal documents and information is not stored on the provided IT infrastructure.	Use of using office equipments for personal purposes.	Sample data 3 to 5% of the machines to be checked documents like CVs, pictures, flash applications etc.
		Applications Development		
27	**A**	Ensure that the modifications etc. being made to the existing reports / software / applications are properly validated by business owners before effecting the changes.	Incorrect outputs of software / reports / application can result in system crashing / behaving erratically, customer dissatisfaction & misreporting.	Review of Application Development process.
28	**A**	Review the Change control process to ensure that changes to programs after their implementation are properly reviewed, approved,	Incorrect outputs of software / reports / application can result in system crashing / behaving erratically, customer dissatisfaction & misreporting.	Review of Application Development process.

Checklist for Information Technology				
S.No.	Priority	**Particulars**	**Risk Associated**	**Methodology**
		documented and tested.		
29	**A**	Ensure that testing of a patch / fix is done in test environment only and its results are properly documented.	Incorrect outputs of software / reports / application can result in system crashing / behaving erratically, customer dissatisfaction & misreporting.	Check for the existence of development / test environment.
30	**A**	All development is done on the development servers only and not on production servers.	Incorrect outputs of software / reports / application can result in system crashing / behaving erratically, customer dissatisfaction & misreporting.	Check for the existence of development / test environment.
31	**B**	Appropriate Version control mechanisms are put in place.	Previous history of any development would not be available for review	Review of the logs & processes.
32	**B**	Applications are released only after appropriate Quality Control procedures have been taken into considerations.	Unchecked software / application can result in system crashing / behaving erratically, customer dissatisfaction & misreporting.	Review of Application Development process.
33	**A**	Release of applications must be done by superior officers	Unchecked software / application can result in system crashing / behaving erratically,	Review of Application Development process.

Checklist for Information Technology				
S.No.	Priority	**Particulars**	**Risk Associated**	**Methodology**
		through a formal process only.	customer dissatisfaction & misreporting.	
		Application Management		
34	**A**	To ensure that the users are not able to directly access and modify the database using tools like SQL & TOAD. Any modifications should be done in the application software and not the database.	Anybody can modify the data in tables without adhering to relationships. On the other hand the application will ensure data consistency is maintained and changes are made on all tables simultaneously.	Check on the Firewall whether the SQL and Toad Port is restricted or not else there should be command inserted in the database to kill any user trying to do so. This can be checked by attempting in such a manner. Audit tools can also be used.
35	**B**	Ensure that auditing feature & security auditing feature is enabled in Oracle database & routers respectively.	This will enable to log every activity on the database but generally not recommended due to performance and storage issues. Therefore a "On demand" basis is recommended.	Review the options and logs on the database server, if not there then check for the existence of "On demand" process.
		Personnel		
36	**A**	Ensure there is adequate segregation of duties and functions in the IT department in respect of areas	There would be no accountability.	Review the KRA mechanisms, JDs and interview for daily job functions.

Checklist for Information Technology				
S.No.	Priority	**Particulars**	**Risk Associated**	**Methodology**
		such as Application programming, Systems programming, Operations, Control and reconciliation of processing input and output, Control of master and data files, Maintenance and up-gradation of IT infrastructure such as PCs, Servers, Network and other peripheral devices.		
37	**B**	Ensure that IT department reports to senior management allowing the department to maintain objectivity and independence from source or user departments.	Independence of the function may be compromised.	Review HR policies and SLA.

Checklist for Information Technology				
S.No.	Priority	**Particulars**	**Risk Associated**	**Methodology**
38	**B**	Review Administrative and operational procedures established within the IT department to ensure that issues such as comprehensive written job descriptions, published policy and procedures manual, rotation of duties of personnel, formal activity logging and review procedures, formal forms control and record retention procedures, physical security of IT department, formal disaster recovery plan including backup facilities and testing procedures, storage and up-gradation of Users Manuals, all software licenses and new system	Leads to dependence on resources.	Review all IT processes related to shifts, JDs, Documentation, Backup etc.

Checklist for Information Technology				
S.No.	Priority	**Particulars**	**Risk Associated**	**Methodology**
		rollout processes etc. are properly addressed.		
		Security Infrastructure		
39	**A**	Corporate Network Security Policy Compliance is met.	Any deviance would lead to intrusions.	Check IT processes with security policy.
40	**B**	Review the security policy of the unit and ensure that none of the users should be allowed more than one login. To also ensure that group login is not allowed.	Accountability in case of unauthorised access cannot be fixed, exceptions can be made only in case of call centers where it is shared.	Multiple login option is disabled.
41	**A**	To ensure that the anti-virus program is installed on all PCs and is updated automatically on a daily basis. Ensure that the anti-virus program is also installed on standalone PCs	Corruption / loss of crucial data.	Anti-virus program is loaded on all the machines and the updates are done through the server I.e. no user intervention required for updating-

Checklist for Information Technology				
S.No.	Priority	**Particulars**	**Risk Associated**	**Methodology**
		and updated regularly with newer versions.		
42	**B**	To ensure that local TCP / IP filtering techniques are used for systems.	Unknown ports and services can be backdoors for Hackers.	Ensure that the unwanted ports are blocked either on the Firewall or individual system level. This can be done through a network auditing tool.
43	**A**	Ensure that the following features are disabled to increase router security – finger service, IP source routing & BOOTP server service.	The finger service lists usernames that are logged into a network device and is therefore useful to the attacker. The ip source routing allow hackers to define their own routes on the network. The BOOTP server disables the hacker to download a copy of router's IOS software.	This should be disabled. Check router configuration files.
44	**A**	Ensure that access list filters are implemented to filter traffic & restrict access to router services.	Unwanted services will leave the network vulnerable.	Checking router configuration files against the wanted and unwanted services.
45	**A**	Ensure that testing of effectiveness of firewalls is done on a periodic basis.	The firewall will be vulnerable to new intrusions.	Process of testing firewall should be in place. Latest Service Packs & versions are installed both on operating systems & firewall package.

Checklist for Information Technology				
S.No.	Priority	**Particulars**	**Risk Associated**	**Methodology**
46	**A**	Ensure that intrusion detection systems are installed at the firewall level to highlight network hacking attempts.	Hacking / intrusion into the network will go undetected.	Intrusion detection systems are installed and their alerts are actioned upon.
47	**A**	Ensure that SYN Defender parameters to protect internal systems from denial of service attacks is activated.	A SYN attack works by overwhelming the victim with requests from a non-existent IP address. The victim responds but does not receive reply, leading to a flood of open connections. These requests may slow down or crash the OS.	This should be disabled. Check router configuration files.
48	**B**	Ensure that the security configuration of servers is updated to protect against known vulnerabilities.	Known vulnerabilities of the systems can be easily exploited by hackers.	Systems are updated with the latest patches / service packs.
49	**B**	Ensure that unsecured communication protocols like FTP &telnet are disabled on servers.	Unsecure FTP and Telnet are open and vulnerable connections.	Check the router configuration and ensure that the communication is encrypted.

Checklist for Information Technology				
S.No.	Priority	**Particulars**	**Risk Associated**	**Methodology**
50	**A**	Ensure that the value of TCP_STRONG_ISS in servers is changed from the default value of "1" to a more secure value to prevent IP Spoofing.	This can cause IP spoofing and make system vulnerable to intrusion.	The value should be set to 2.
51	**A**	Ensure that redundant "aux" parameter is removed from the router configuration.	The aux parameter allow people to access through dial-ups.	This should be disabled. Check router configuration files.
		Physical Security		
52	**A**	Ensure that access to computer hardware, programs, program documentation, data files and server is limited to authorized personnel only.	Unauthorised access to IT resources, which can result in hardware & data theft.	Server room / data centre should have access control mechanism open to only relevant users.
53	**A**	Reprographics room is under a secured environment and access to devices such as printers, fax machines,	Unauthorised transfer of data to outside sources.	Check Physical access control mechanisms.

Checklist for Information Technology				
S.No.	Priority	**Particulars**	**Risk Associated**	**Methodology**
		photocopiers, dak section have access control mechanisms.		
	B	Ensure that the network diagrams are not displayed in the organisation, where visitors have access.	Security of the network can be compromised.	Network diagrams should not be displayed in the areas where visitors have access.

II. Checklist for Statutory & Regulatory compliances

Checklist For Statutory & Regulatory Compliances –Telecom					
S. No.	**PRIORITY**	**QUESTIONNAIRE**	**RISK ASSOCIATED**	**METHODOLOGY**	**INPUT REQUIREMENTS**
1.	A	Whether reports such as Performance Monitoring & Quality of Service Report, Tariff Report, Inter-Connection Reports etc., required to be submitted to the various regulatory authorities such as DOT, COAI, TRAI etc. are sent in prescribed format & on scheduled dates.	Penalties/ legal proceedings may follow if these Reports are not submitted/ late submitted.	**1. Check the formats of the reports submitted to DOT etc. with the formats given in Annexure- I** **2. Also, check whether the reports have been submitted within due time limits.**	Obtain the submission acknowledgements of the Performance Monitoring & Quality of Service Report, Tariff Report, Inter-Connection Reports etc. which had been submitted to DOT etc.
2.		Whether the figures reported in such	In case incorrect figures reported to	**Check the figures given in the reports**	**Obtain the concerned base**

Checklist For Statutory & Regulatory Compliances –Telecom					
S. No.	**PRIORITY**	**QUESTIONNAIRE**	**RISK ASSOCIATED**	**METHODOLOGY**	**INPUT REQUIREMENTS**
		Reports tally with the Circle MAPA & financial books.	DOT etc., legal consequences/ penalties may follow.	**with the base documents.**	**documents**
3.		Ensure that the licenses to operate are obtained / renewed at the required time / frequency.	Non-compliance will amount to illegalized operations	Examine whether the license to operate has been duly received before the start of operations. Check in case of expiry of license, whether renewal has been timely done.	Obtain the copy of the license to operate
4.		Is there a system in place to maintain/ preserve all notices/ correspondences from DOT/ other regulatory authorities	Lack of preservation of these notices may result in important notices / queries remaining un-responded.	Check whether all the notices/correspondences have been preserved date wise since beginning and a control register is maintained with details like receipt date, nature of notice and when responded etc.	Obtain the register and file of all the notices/ correspondences from various authorities.
5.		Is there a proper system of responding to such notices/ correspondences?	Penalties/ legal proceedings may follow.	1. Check whether they have been replied in accordance with corporate guidelines attached in Annexure- 2. 2. Check the timeframe within	Obtain all the responses/ clarifications sent by the Circle.

Checklist For Statutory & Regulatory Compliances –Telecom					
S. No.	**PRIORITY**	**QUESTIONNAIRE**	**RISK ASSOCIATED**	**METHODOLOGY**	**INPUT REQUIREMENTS**
				which it is responded to?	
6.		Ensure that the basis of calculation of regulatory charges such as Fees for Revenue Sharing etc., are correct & accordingly such dues have been duly paid within stipulated time.	Excess/ wrong payment of Fees for Revenue sharing resulting in loss of funds while short payment will lead to interest payments.	1. Understand how the calculation for Fees for Revenue Sharing is to be done & ensure that such calculations have been made accordingly. 2. Check whether it has been paid within such timelines.	1. Working papers for calculation of amount of Fees for Revenue Sharing etc. 2. Obtain the timelines within which such charges are to be paid
7.		Ensure that the original copies/ photocopies of all the Government approvals of a regulatory nature such as SACFA clearances for ROW, PCM links and frequency allocations etc. are physically available and properly maintained.	Lack of these approvals will weaken our stand in future legal proceedings.	Examine whether all the copies are physically available & properly maintained with the Circle.	Obtain original/ photocopies of all the government approvals of a regulatory nature.
8.		Ensure that clearances from Municipal Authorities such as	Non-availability of these clearances may lead to disputes / problems from	1. Match the clearances obtained from Municipal authorities with the	1. Obtain a list of all the sites 2. Original/ photocopies of

Checklist For Statutory & Regulatory Compliances –Telecom					
S. No.	**PRIORITY**	**QUESTIONNAIRE**	**RISK ASSOCIATED**	**METHODOLOGY**	**INPUT REQUIREMENTS**
		MCD, NDMC, PWD, DDA etc. are obtained & properly preserved for all the sites at various locations. Also whether structural stability certificate, building bye laws conformances etc. obtained.	these agencies.	list of all the sites & identify the ones for which clearance has not been obtained. 2. Also check whether structural stability certificate, building byelaws conformances etc. had been obtained for all the sites.	clearances from Municipal authorities for various sites.
9.		Ensure that lease / leave and license agreement is duly entered into for all cell sites.	Lack of our stand against any future legal proceedings for setting up these sites.	Match the list of all the sites with the leave & license agreements obtained for them and identify the sites for which it has not been obtained. Also check for the validity and completeness of these agreements.	Original/ photocopies of all the leave & license agreements entered into for various sites.
10.		Ensure that original copies of all the agreements with roaming partners, vendors and suppliers, Business partners etc. are physically available and properly maintained for legal	Lack of these agreements will weaken the stand in future legal proceedings.	1. Check if agreements have been entered into with all the roaming partners. 2. For agreements with suppliers, obtain a list of suppliers for which agreement have been entered & check if	1. Obtain a list of all the roaming partners & a list of suppliers with which an agreement has been entered with the 2. Original/

Checklist For Statutory & Regulatory Compliances –Telecom					
S. No.	**PRIORITY**	**QUESTIONNAIRE**	**RISK ASSOCIATED**	**METHODOLOGY**	**INPUT REQUIREMENTS**
		compliance.		copies of all such are with the Unit.	photocopies of agreements with roaming partners, suppliers etc.
11.		Whether all The agreements entered into by the Circle are valid in law i.e. on adequate value of stamp paper & the date of agreement within the validity date of the stamp paper etc.	Agreements entered into but not a valid document in law.	Review all the agreements to check • All agreements are vetted by the legal department • Agreements are on adequate value stamp paper • Agreement date is after the stamp paper date • The agreement date is within the validity date of the stamp paper • Alterations in the terms of the agreement are properly executed & countersigned. • All expired agreements are renewed in time	Original/ photocopies of all the agreements entered into by the Unit.

Checklist For Statutory & Regulatory Compliances –Telecom					
S. No.	**PRIORITY**	**QUESTIONNAIRE**	**RISK ASSOCIATED**	**METHODOLOGY**	**INPUT REQUIREMENTS**
12.		Ensure that various provisions of Income Tax are duly adhered to • Calculation of amount of TDS in respect of payments for salaries, contractors, professional fees, rent, brokerage etc. • Deposit of TDS within stipulated time • Proper Receipt & issue of TDS Certificates • Returns to be filed with Income Tax Authorities are duly filed & within timelines.	Imposition of penalties under Income Tax Act.	1. Check the computation of rate of TDS for all the payments made for salaries, contractors, professional fees, rent, brokerage etc. 2. Check from the TDS Challan, whether it has been submitted within due time. 3. Check whether Consolidated TDS Certificates has been timely received & issued.	1. Ledger for salary, contractor etc. for the period 2. Original copies of TDS Challan. 3. TDS Certificates issued & received.
13.		Ensure that various provisions pertaining to Provident Fund, ESI & Gratuity are duly adhered to.	Imposition of penalties under various laws.	1. check for Correct Deduction & timely deposit of PF, ESI & Gratuity. 2. Check for Deduction of PF on payment of leave Encashment for existing	1. Basic salary for all the employees on the payroll of the company. 2. Original Challans for deposit of PF,

Checklist For Statutory & Regulatory Compliances –Telecom					
S. No.	**PRIORITY**	**QUESTIONNAIRE**	**RISK ASSOCIATED**	**METHODOLOGY**	**INPUT REQUIREMENTS**
				employees. 3. Check for Filing of Returns/ forms relating to PF, ESI within stipulated time.	ESI & Gratuity. 3. Returns filed for PF, ESI.
14.		Ensure that compliance of PF, ESI & various labour laws in case of labour employed by the Contractor are duly adhered to.	Although labour employed by the Contractor but because of non-compliance of various laws, penalties could be imposed on Bharti.	Examine the copies of Challans of PF etc. as a proof of deposit for the workers employed by contractor for Bharti.	Copies of PF etc. Challan from the contractors.
16.		Ensure that various provisions pertaining to Shops & Establishments Act, Payment of Bonus Act, Registration Act & other labour Laws duly adhered to.	Imposition of penalties under these laws.	Examine the compliance statement & verify if it is correct.	Obtain the compliance statement.
17.		Ensure that the quarterly return in Form ER I and biannually return ER II are submitted before the due dates as specified in Employment Exchanges	Imposition of penalties under these Rules.	Verify whether it has been prepared correctly and submitted within specified time.	Obtain the quarterly return submitted as per Employment Exchange rules.

Checklist For Statutory & Regulatory Compliances –Telecom					
S. No.	**PRIORITY**	**QUESTIONNAIRE**	**RISK ASSOCIATED**	**METHODOLOGY**	**INPUT REQUIREMENTS**
		(Compulsory Notification of Vacancies) Rules, 1960.			
18.		Whether the transactions involving foreign exchange has been made meeting all the statutory requirements.	Imposition of penalties under these laws.	Identify the transactions made in foreign exchange & if check all the statutory requirements of FEMA & RBI guidelines are duly met.	Obtain the schedule of inflows & outflows made in foreign exchange.
19.		Ensure in the case of following • Office Premises – whether building plan sanction, completion certificate etc. are properly obtained • Advertising Banners / Hoarding – whether approval from municipal corporation / PWD etc. is duly obtained	Lack of these documents will weaken our stand in future legal proceedings.	Check if the office premises the Building plan sanction, completion certificate etc. are timely obtained & properly maintained.	Obtain the original/ photocopies of various approvals/ sanctions received for office premises & for advertisement banners, hoardings etc.

Checklist For Statutory & Regulatory Compliances –Telecom					
S. No.	**PRIORITY**	**QUESTIONNAIRE**	**RISK ASSOCIATED**	**METHODOLOGY**	**INPUT REQUIREMENTS**
20.		What is the amount of fines/ penalties imposed during the period • Analyse the reasons for such levy & whether it was avoidable. • What are the chances of imposition of this penalty/ fine again?	Same mistake repeating again resulting in re-imposition of penalties which are avoidable.	1. Examine the schedule of expenses & identify if there are some fines/ penalties imposed. 2. Check the assets accounts wherein some penalties may have been included in the total cost and capitalised. 3. Enquire the reasons for the same & examine if there are some steps taken so as to minimize its re-occurrence.	Obtain the expense schedule for fines & penalties.
21.		Whether the payment for expenditure of electricity connection at cell sites is timely made & ensure no extra amount is charged.	Penalties/ legal proceedings in case of non-compliance.	Verify the following for the electricity connections at cell sites: • State Electricity Board clearances are obtained. • Check the proof of payment of the dues in case the meter is in the	Obtain a copy of the clearance from State Electricity Board. Obtain copy of electricity bills paid in the past along with the supporting bills and proof of payment.

Checklist For Statutory & Regulatory Compliances –Telecom					
S. No.	**PRIOR ITY**	**QUESTIONNAIRE**	**RISK ASSOCIATED**	**METHODOLOGY**	**INPUT REQUIREMENTS**
				name of the Landlord. • Check if the payment Is made within due time & no penalty is imposed because of late payment • Check that the rates charged by the Electricity Board to the landlord are for commercial use and not for residential usage. • Check if the reading of the meter tallies with the amount billed by the Electricity Board.	
22.		Whether all provisions of The Customs Act are duly complied with	Penalties levied which could have been avoidable.	1. Examine all notices/ proceedings with the Customs department are timely & properly followed. 2. Review the reasons for the payment of demurrage paid & identify if it was	Obtain a copy of the relevant documents for all proceedings with the Customs department

Checklist For Statutory & Regulatory Compliances –Telecom					
S. No.	**PRIORITY**	**QUESTIONNAIRE**	**RISK ASSOCIATED**	**METHODOLOGY**	**INPUT REQUIREMENTS**
				avoidable. 3. Enquire the reasons for any penalty levied	

****

Chapter 23
Audit Follow-up

The Institute of Internal Auditors definition of a follow-up: "A follow-up is defined as a process by which the internal auditors determine the adequacy, effectiveness and timeliness of actions taken by management on reported audit findings."

The value of the audit must be assessed to assure that the findings and recommendations, reflecting cost conscious, workable and timely solutions, have been achieved to some quantifiable degree and provide value to the organization. Unfortunately, this does not happen as often as it should in practice. More organizations would not outsource their audit function if they gained a thorough understanding of the savings and improvement to operations and processes the audit can bring.

The bottom line is how does audit enhance an organization's value? Follow-up is the answer, if an organization is to understand what value audit can have to improving operational integrity, efficiency and effectiveness. By looking at the prior audit recommendations of earlier work, auditors are able to assess if the agency, company or corporation has taken any action toward the report recommendations. If it has, a process is in place to try to assess what impact those recommendations had and to formally report the assessment and findings. Often, auditors will receive direct feedback from managers, supervisors or staff that their actions were the results of an earlier audit report. In some instances, they may even provide direct information and cost figures on how much is being saved as the result of new controls in place or improvements to the existing processes.

Where agreed action plans are not completely implemented the auditor asks the following questions:

What remains to be done?

By whom and when?

Have alternatives been implemented that may be more appropriate?

Has the agreed action plan ceased to be of value?

If no action was taken, why not?

What is the issue or concern causing inaction?

The end result should be a brief summary of the status of every action plan agreed upon. The final summary is reviewed with the person responsible for clearing the audit report before the follow-up report is issued.

****

References

1. http://en.wikipedia.org/wiki/Internal_Audit#cite_note-6
2. http://www.qfinance.com/auditing-best-practice/aligning-the-internal-audit-function-with-strategic-objectives?page=1
3. HTTP://WWW.QFINANCE.COM/AUDITING-BEST-PRACTICE/ALIGNING-THE-INTERNAL-AUDIT-FUNCTION-WITH-STRATEGIC-OBJECTIVES?PAGE=1
4. www.trai.gov.in
5. www.dot.gov.in
6. KPMG Internal_audit_role
7. http://usf.usfca.edu/internalaudit/pdf/USF_%20IAManual.pdf
8. http://www.iia.org.uk/about-us/what-is-internal-audit
9. http://www.theiia.org/guidance/standards-and-guidance/ippf/definition-of-internal-auditing/?search%C2%BCdefinition
10. http://www.audit.cornell.edu/faq.html#internal_auditors
11. http://www.metricstream.com/insights/bestpractices_intaudit.htm
12. http://www.ehow.com/how_6565214_design-audit-checklist.html?ref=Track2&utm_source=ask