CA.RAKESH CHOUDHARY,B.SC.,MIMA.,MICA.,FICWA.,FCA

CHARTERED ACCOUNTANT

BANK AUDIT

GREAT INDIA

2011 New Edition

BANK AUDIT

ANNUAL AUDIT OF BANK
CONCURRENT AUDIT
REVENUE AUDIT
STOCK AUDIT
DEBTORS AUDIT
CREDIT AUDIT
TAX AUDIT
LONG FORM AUDIT REPORT
With Introduction to IFRS,AAS,IGAS,SIA and Important Checklists

"Annual Audit of Bank Branches is an annual exercise of Auditing the Financial Statements,Financial Reporting,Internal Control,Fraud Control,NPA Management of the bank branch and the development of the bank and the country's economy." -

CA.RAKESH CHOUDHARY,B.SC.,MIMA.,MICA.,FICWA.,FCA

CHARTERED ACCOUNTANT

Authors' Foreword

The Members of the Institute of Chartered Accountants of India

Dear Members and Students of ICAI *15.03.2011*

A Happy Annual Bank Audit

As you are in the process and preparation for Annual Audit, Concurrent Audit, Revenue Audit,Stock Audit,Debtors Audit,Credit Audit,Tax Audit,LFAR, etc of Bank Branches with introduction to IFRS,AAS,IGAS & SIA and Important Checklists it is a small endeavour from me by writing a book on Annual Audit of Bank and introduce you to the intricacies of Annual Audit of Bank Branches in India.I have tried to elucidate the Audit Plans,Programs,Procedures and Policies to be adopted during the process of Annual Audit of Bank branches in India.The process starts from the appointment of Auditors,acceptance and signing off of all the Statements,Certificates and documents, LFAR,Tax Audit u/s 44AB as per guidelines of the Reserve Bank of India,Institute of Chartered Accountants of India,Bank norms and Government of India.

The book contains all forms of Audit Report,Management representations,Engagement Letters,Audit Sampling,Models,Documents required from the branches,Audit programs,RBI notifications,Accounting Standards,Auditing and Assurance Standards,Statistical Quality Controls,IFRS,GASAB,Standard on Internal Auditing(SIA) etc for your convenience in conducting the Annual Audit of Bank,Concurrent Audit, Revenue Audit,Stock Audit,Debtors Audit,Credit Audit,Tax Audit,Long Form Audit Report etc.

The book has been written taking into account the reference guidelines issued by The Institute of Chartered Accountants of India.

The book also contains a questionnaire on Compliance of AAS 28 i.e Auditing in a Computerised Information Systems environment to implement Information Systems Audit,Concurrent Audit,Revenue Audit,Stock Audit,Debtors Audit,Credit Audit,Tax Audit,Long Form Audit Report etc of the Bank branch.It also gives an idea about fraud controls and internal controls required by the Bank Branch which the Statutory Auditor has to Audit and Report on the same.

Hope all the members enjoy reading the book,implement and conduct Audit incorporating all the guidelines given in the book and very useful for auditors of the bank branch and the banks.All suggestions,comments and discrepencies are invited from the members of The Institute of Chartered Accountants of India,Bank Managers and readers of the book.

Thanking you,

Sincerely Yours; and

with Regards

CA.RAKESH CHOUDHARY,B.SC.,MIMA.,MICA.,FICWA.,FCA

CA.RAKESH CHOUDHARY,B.SC.,MIMA.,MICA.,FICWA.,FCA

CHARTERED ACCOUNTANT

BANK AUDIT

GREAT INDIA

HIGHLIGHTS

STATUTORY BANK BRANCH AUDIT

AUDIT ENGAGEMENTS,DOCUMENTATION,INTERNAL CONTROLS,FRAUD CONTROLS,AUDIT REPORTS,

INFORMATION SYSTEMS AUDIT,AUDIT PLANS & PROGRAMS,AUDIT CERTIFICATES,CORPORATE GOVERNANCE,QUALITY CONTROL STANDARDS,AAS,MANAGEMENT REPRESENTATION AND SAMPLING etc.

RBI NOTIFICATIONS TILL DATE i.e 15.03.2011

INTRODUCTION TO IFRS

AUDITING AND ASSURANCE STANDARDS

CONSULTATIVE PAPERS ON BASEL III (BIS)

CHECKLISTS AND AUDIT DOCUMENTS AND PAPER ON VARIOUS BANK AUDITS

TAX AUDIT

CONCURRENT AUDIT

REVENUE AUDIT

BRANCH AUDIT

CREDIT AUDIT

DEBTORS AUDIT

LONG FORM AUDIT REPORT

STOCK AUDIT

VARIOUS MODELS ON BANK AUDIT

AUDIT OF BORROWERS

AUDIT IN A COMPUTERISED ENVIRONMENT-AUDITINF AND ASSURANCE STANDARDS- AAS 28

AUDIT PLANS AND PROGRAMMES

BALANCE SHEET OF A BANK

BANK FINANCIAL STATEMENTS AND FINANCIAL REPORTING AS PER IFRS – A MODEL

OTHERS

TOTAL PAGES OF THE BOOK – 600 PAGES

Contents

Chapter 5

Audit of Banks Operating in a Computerised Information Systems Environment

Compliance of AAS 28-Auditing in a Computerized Information Systems Environment

Name of the Bank:

Particulars of Branch:

Period during which Audit/Review was carried out: AS ON 31ST MARCH 20... (20....-.....)

Review carried out by: CA.RAKESH CHOUDHARY

1. *General understanding*

1.1 Please furnish an overview of the CIS environment prevalent in the bank, indicating separately each software application used by the bank/branch at any time during the year under review (for example, if the bank used a core banking solution along with separate ATMs, Internet banking software application, set out the CIS environment for each of these, the period for which each software is being used etc).

1.2 Were different versions of the software used by the bank/branch during the year? If so,furnish details for each item of such software.

1.3 Did the bank migrate from an earlier legacy system to the current system during the year? If so, furnish details of the old software, and date of migration.

1.4 Please furnish an overview of the hardware environment available with the bank/ branch,the details of the relevant manufacturers,the date from which each item is being used.

1.5 Has the bank carried out any IS audit during the year? If so, summarise the scope of the review, the period covered, their salient observations and the corrective action taken by the bank as a result thereof.

1.6 Summarise observations of previous statutory auditors/internal inspectors/ concurrent auditors/RBI relevant for the current exercise.

1.7 List out areas/activities/transactions instruments which are handled manually or outside system. How is each such item handled?

1.8 Are there documented procedures available for all activities to be carried out by the data Centre/IS department?

1.9 Are there user manuals available for each item of application software at bank /branch? Are they current and up-to-date?
1.10 What are the functions of each person in the IT department/data centre.
1.11 Is system administration and business application administration kept as separate activities?
1.12 Does the bank provide Internet banking facilities? Did the bank obtain the approval of the Reserve Bank of India before offering such facilities?
1.13 Set out briefly interfaces available between different sets of software and data movement from one to another.

2. Application Software (To be prepared separately for each application software)

2.1 Authentication

a. When a new user is created in the system,who generates the default password and is this forced to be changed on first login?
b. How is the password generated communicated to the end-user?
c. How are passwords transferred in the application to the database?
d. Is there a password policy; If so, are users aware of the same?
e. Can passwords be reused, if so at what frequency?
f. Are number of changes to password in a day restricted?
g. Are one-way hashes or any other encryption used to store and compare the passwords?
h. Are entered passwords decrypted to be compared with the one stored in the database?
i. What is the min & max length of passwords? Are they case sensitive? Can user names and passwords be the same?
j. How is password loss handled?
k. Are the user details encrypted in the database?
l. Does the system lock out users on ‘x’ number of login attempts? If so, how is the same controlled by the Application administrator?
m.Is the session expiry time and other authentication related parameters configurable?
n. Are failed login attempts logged?
o. Is the previous login information flashed on login?
p. Does it show the duration of the session?
q. How are administrator’s details managed? How are the details managed when a system or application administrator is on leave?
r. How user records of those who have quit or transferred are handled in the application?
s. Is remote access to applications provided? If so, how are security issues are handled? If remote access is provided, are there any secure communication channel established?

2.2 *Access Control*

a. Are user groups maintained? If so, are access rights granted at the group level or at an individual user level? And how are read/write access given to a module?
b. Is there a maker-checker process in place? If so, set out details
c. How is maker-checker met when the assigned checker is not available?
d. Does the system allow auto authorise?
e. Obtain a matrix setting out the authorisation limits for accessing each module (data entry,verify, cancel, reverse, view)
f. Can software applications be accessed during holidays and non-working hours?
g. Are there any EOD and BOD operations?
h. Can a transaction be input after the EOD and before BOD?
i. Please furnish major activities carried out during EOD and BOD.
J. Is application access logged? How often this log is reviewed for any intrusions?

2.3 *Data Security*

a. What is the security provided to the database?
b. How does the application access the database?
c Can users access the database using any other utility or directly?
d. How are temporary users handled in the system?

2.4 *Data Integrity*

a. What are the back-end changes that have been made in applications? Is there a record of changes made, date of change, person who authorised the same, person who made the change, table readings before and after the change?
b. Have you procured all available documents in this respect and reviewed them?
c. Are back end changes resorted to occasionally with adequate reasons or are there a number of them indicating a larger problem?
d. How is transmission of sensitive information handled in the systems?
e. Are any standard encryption algorithms used for the same?
f. Are all user activities logged?
g. How are adjustments/corrections, if any, handled in the applications?
h. Does the testing area application is in sync with the production area (which includes the application software, any middleware, database objects, reports etc)?

2.5 *Audit Logs*

a. Are all changes to master information captured and logged in the system?
b. Please set out briefly all audit logs available in the system.
c. Have you reviewed changes to master information carried out during the year and are you satisfied that they are in order?
d. Have you verified all changes to interest and tax masters with reference to circulars received from central office along with the date of their validity?

2.6. *Testing*

a. Did the bank carry out a formal testing of all new software/versions of the same before being incorporated into the production environment?

b. Have you reviewed the test cases, the expected results document and the results generated from the new system to ensure their accuracy and consistency?

c. Are the test and production environment clearly segregated and demarcated?

d. Were formal signoffs issued for each item of new software/version?

e. What are the known bugs in the software/functionality and how are these controlled?

f. What change requests are pending completions from the software vendor? Do any of these reveal any bugs or deficiencies in the application software?

g. Are there any documented procedures for change requests, change management, release to test area from development and release to production area from test environment?

h. How are failures in EOD/BOD handled?

I. Are there multiple resources authorised to run the EOD/BOD?

j. Are there any unprocessed transactions outstanding as at 31st March 20...? If so give details and how are they proposed to be handled?

2.7. *Accounting Entries*

a. Summarise all system generated entries.

b. Have you reviewed the scheme of accounting entries passed by the system to ensure their correctness?

c. Are there any value or back dated entries and what is the mechanism to control the same?

d. Is there a record of all value or back dated entries?

e. Can value or back dated entries be passed for a closed accounting period?

f. Is it possible to reconcile balances in accounts prior to and post passing of value dated entries?

g. Take a sample of entries passed by the system and verify its calculations and correctness(particularly calculations of interest/fees paid or charged. While selecting sample of accounts to be verified, please ensure that all types of loan and deposit accounts are covered- fixed deposits, FCNR, NRE, RFC, recurring deposits, cumulative deposits,term loans, term loans where repayments are made by EMI, cash credit, PC, PCFC, bills,foreign bills, LCs, bank guarantees etc. Sample must cover cases where payment of interest/installment, receipt of stock statements etc are delayed). Document the same. In case an audit of treasury is involved, all calculations of profit/loss on sale of securities,pay outs on derivatives etc are to be test verified.

2.8 *Data migration*

a. If data has been migrated from any legacy system during the year, have you reviewed the migration process?

b. Data migration - Is this done manually or through application utilities? If through application utilities, have these utilities been tested to ensure correctness of the data migration process and accuracy of data.

c. Have you reviewed the pre and post migration reports to ensure consistency and integrity of data migrated to new system?

d. If any data was not available in earlier legacy system, explain the process by which they were collected and input into the new system.

e. Was there a parallel run before which the new system went live?

f. What are the issues and problems still pending in the post live environment?

3. *IT Infrastructure at the bank : Network & RDBMS Security*

a. Who creates the user accounts and assigns folder access rights?

b. How are users groups maintained and ensured not part of sensitive groups like root,system etc.

c. What is the frequency of password change?

d. Is there a password policy if so what is it?

e. How is the creation or deletion of a network user account managed e.g. when an employee quits the organisation or transferred?

f. Is there a validity associated with each user account?

g. How are vendors/visitors from other branches (e.g. head office) provided access to the network?

h. Have Default passwords of RDBMS and applications been changed?

i. How are the RDBMS and Server Space monitored and administered to prevent crashes?

j. On what basis are roles organised in the RDBMS from a security perspective?

k. Are any system administration utilities used?

l. What are the precautions taken against viruses? How and what is the process of ensuring latest DAT files are updated on all servers, desktops, laptops? Are these being monitored?

m.Can you please share the guidelines on users from the computer policy and planning department (CPPD)?

n. Spy ware,adware, malware, trojans - What kind of protection is provided to ensure these are not present in the network?

o. Are all hardware equipments, network under maintenance contracts? Are they being serviced,maintained regularly?

p. Perimeter security - How is the bank’s network infrastructure and server infrastructure protected? Has anyone tested the routers, firewall, gateway, bridge configuration parameters?
Has anyone done a penetration and intrusion testing on these? What are the results?

q. How often are the application and the database backed up? What is the backup policy?

Is it daily incremental or daily full? What about weekly backups? Where and how are the tape media stored? Is it stored in an off-site location? Are these tapes tested for backup effectiveness? Are back up logs maintained, monitored, and reviewed?

r. How are end users trained on using the application software? How is it done for new users?How are users trained on new modules / enhancements?

s. Is the tape media life monitored? What happens once a tape reaches its life? How is this tape destroyed? Are there any logs for these?

4. *Business Continuity and Disaster Recovery Plans*

a. What is the business continuity plan of the bank/branch?

b. What are the backup procedures that are in place?

c. Where is the DR site located? Is it in the same building or geographically different location?
How is the live production environment replicated on a DR site? Is this tested regularly? Is this facility manned? What kind of security process is implemented in a DR site? What kind of communication links are provided at the DR site? How is the switch over from the live site to DR site is planned? Has this been tested? How often is this tested? Are these tests documented? Are there any teams responsible for BCP and DR activities?

d. Where are the backups stored, what is the frequency of recycling the tapes,are periodic readability tests performed on the tapes and are logs of the same maintained?

e. What are the service level agreements with vendors and the Information System Department of the bank for uptime of applications?

f. Are all software licensed? How is this monitored? Are there any document / database to monitor licenses? How is software license usage audited?

g. Are vital and statutory documents printed regularly or backed-up electronically?

h. Are databases mirrored?

i. Is there a periodic review of the BCP related activities?

j. In case of server crashes, what is the contingency plan in place?

k. Was there any crash in the computer system during the year? If so, how were the application software and data base restored?

l. Were any consistency checks made before restoring the application software and data base?

5. *Hacking*

a. Were there any reported cases of hacking of the computer systems during the year? If so, please furnish details.

b. Have there been complaints from customers regarding wrong balances/ transactions in their accounts? If so, please furnish details of each of them.

c. Have any frauds or irregularities been detected due to malfunction of the computer systems?

d. Have there been instances where cash as per ATM did not match with books? If so,furnish full details.

6. *Identification of transaction for substantative checking*

a. Use the data available in the computer system to identify large transactions, select a sample,transactions which are outside the mean value by a significant percentage. For this purpose, the data base can be down loaded into excel , which could then be sorted, arranged in ascending/descending order to facilitate identification of transactions which are large or outside the mean value by a significant percentage.

7. *Use of reports generated by system*

a. Before relying on any report generated by the system, carry out validation checks to ensure that the same is complete and correct. This could be done by identifying a sample of transactions, validating them with the base records in the system and cross checking the results arrived at by the system. Do not take all reports which are generated by the system at its face value. There may be bugs or deficiencies in the report generated or there may be interventions by the bank while generating the report (by down loading data to excel and making corrections to certain fields before they are handed over for audit)

b. Are all control accounts and subsidiary ledgers compared and reconciled?

c. Are there any instances of the same data as per different sets of reports being different and inconsistent?

8. *Documentation*

Is all information in electronic form properly indexed, labelled and maintained in a readily retrievable form?

Chapter 18 AUDIT DOCUMENTATION

Audit Plan and Program – Model - I

Annual Audit Appointment Letter

|

Acceptance Letter of Appointment as Auditor

|

Declaration of Fidelity and Secrecy

|

Declaration of Proprietor of the Chartered Accountant Firm in Full Time Practice

|

Declaration of no Dis-Qualification as Chartered Accountant and Auditor as per Section 226 of the Companies Act,1956

|

No-Objection Certificate from Previous Auditor

|

Engagement Letter with Documents to be audited to the branch

|

Management Representation Letter with all documents to be audited

|

Audit of Bank Branch/R.O/Z.O/H.O

|

Auditor's Report

|

Long Form Audit Report

|

Tax Audit Report

Chapter 22 Standard on Internal Audit (SIA)

SIA – 1	Planning an Internal Audit
SIA – 2	Basic Principles governing Internal Audit
SIA – 3	Documentation
SIA – 4	Reporting
SIA – 5	Sampling
SIA – 6	Analytical Procedures
SIA – 7	Quality Assurance in Internal Audit
SIA – 8	Terms of Internal Audit Engagement
SIA – 9	Communication with Management
SIA - 10	Internal Audit Evidence
SIA – 11	Consideration of Fraud in an Internal Audit
SIA – 12	Internal Control Evaluation
SIA – 13	Enterprise Risk Management
SIA – 14	Internal Audit in an Information Technology Environment
SIA – 15	Knowledge of the Entity and its Environment
SIA – 16	Using the work on Expert
SIA - 17	Considerations of Laws and Regulations in an Internal Audit

Chapter 27

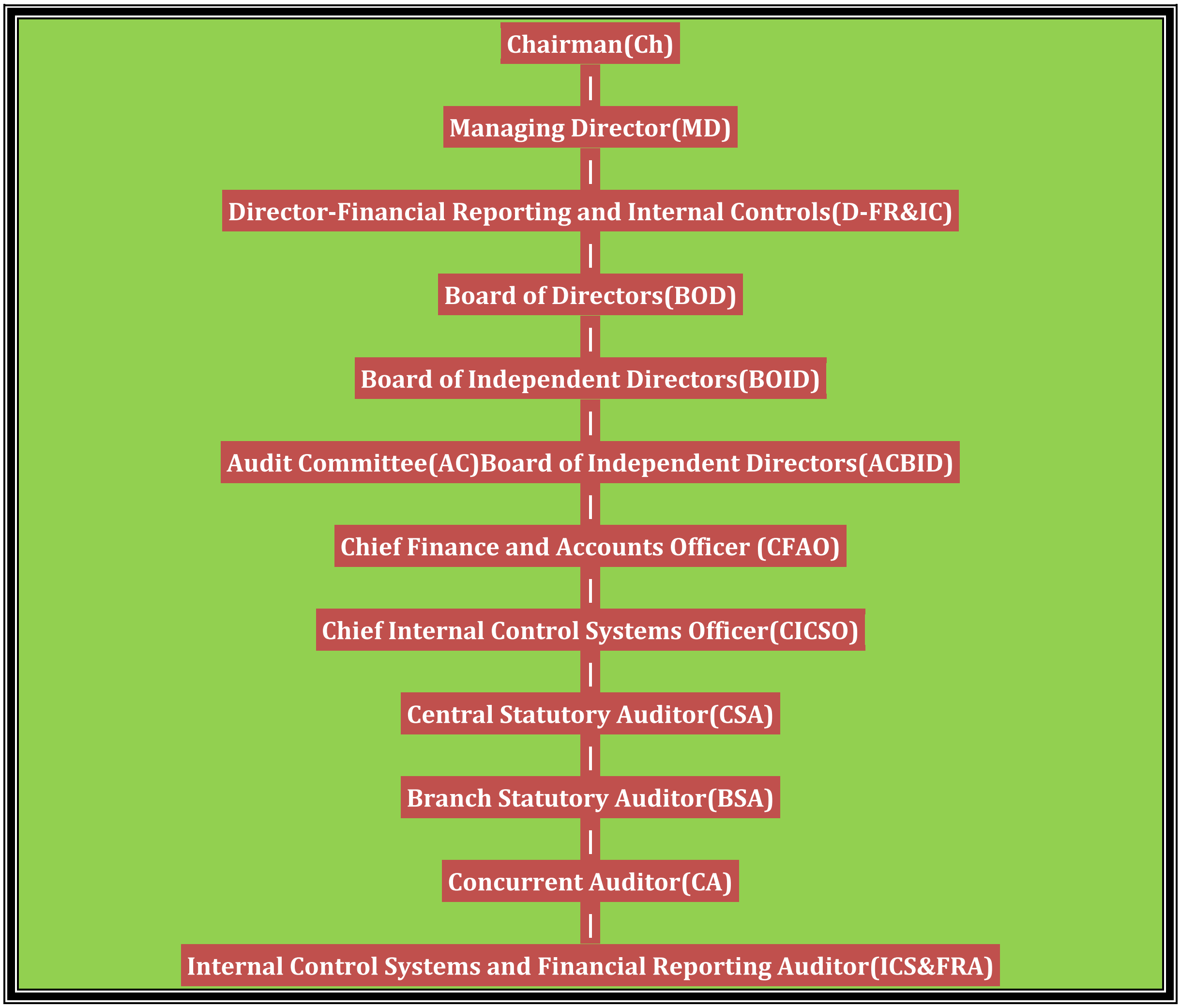
International Financial Reporting Standards(IFRS)

Banks have to prepare their financial statements and financial reporting as per IFRS.

IFRS -1	First Time adoption of IFRS
IFRS -2	Share Based Payment
IFRS -3	Business Combination and Group Reporting
IFRS -4	Insurance Contracts
IFRS -5	Non-Current Assets held for Sale and Discontinued Operations
IFRS -6	Exploration for and evaluation of Mineral Resources
IFRS -7	Financial Instruments-Disclosures
IFRS -8	Operating Statements
IFRS -9	Financial Instruments-Measurement,Recognition &Disclosures

Chapter - 35

Bank Board-Audit-Auditors-Audit Committee Framework – A Model



Chairman(Ch)

Managing Director(MD)

Director-Financial Reporting and Internal Controls(D-FR&IC)

Board of Directors(BOD)

Board of Independent Directors(BOID)

Audit Committee(AC)Board of Independent Directors(ACBID)

Chief Finance and Accounts Officer (CFAO)

Chief Internal Control Systems Officer(CICSO)

Central Statutory Auditor(CSA)

Branch Statutory Auditor(BSA)

Concurrent Auditor(CA)

Internal Control Systems and Financial Reporting Auditor(ICS&FRA)

Chapter - 36

Bank - Audit & Auditors – A Model

Director-Financial Reporting and Internal Controls(D-FR&IC)

|Financial Reporting and Internal Controls

Chief Finance and Accounts Officer (CFAO)

|Finance & Accounts

Chief Internal Control Systems Officer(CICSO)

|Internal Control Sytems

Central Statutory Auditor(CSA)

|Central Statutory Audit

Branch Statutory Auditor(BSA)

|Branch Statutory Audit

Concurrent Auditor(CA)

|Concurrent Audit

Internal Control Systems and Financial Reporting Auditor(ICS&FRA)

|Internal Control Systems and Financial Reporting

Chapter - 41

CERTIFICATIONS OF BORROWAL COMPANIES BY CHARTERED ACCOUNTANTS/ COMPANY SECRETARIES/COST ACCOUNTANTS

- Terms of reference for stock audit are to be spelt out clearly by the Banks,so that the Chartered Accountants can give focused attention to such areas.
- End-use verification of funds lent,if certified by Statutory Auditors,will be a good comfort to the Banks.
- As Banks quite often deal with unlisted companies,disclosure requirements for such companies above a specific turnover may be made akin to those for listed companies, viz. consolidated balance sheet, segmental reporting etc.
- Information on large shareholding also will be useful.
- The following additional certification either from Chartered Accountant or Company Secretary or Cost Accountants may also be thought of :-
    - Company Directors not figuring in defaulters list (RBI/ECGC)/willful defaulters list etc.)
    - Details of litigation above a specified cut off limit.
    - A specific certificate,probably from the Company Secretary,regarding compliance with Sec. 372 (a) of the Companies Act.
    - Details of creation/ modification/satisfaction of charges on the assets of the company, position regarding insurance,show cause notices received, finds and penalties awarded.
- As regards rotation of Auditors,for the sake of operational convenience,it is suggested they may be changed once every 5 years instead of every 3 years.
- In order to avoid concentration, group companies may have different Statutory/ Internal Auditors in case group turnover exceeds Rs.100 crores.