

# Manual of Information Technology Audit

## Volume II

Checklists for field audit  
parties

Office of the Comptroller &  
Auditor General of  
India

## Check lists for field audit parties

### Table of Contents

<b>Sl. No</b>	<b>Particulars</b>	<b>Page No.</b>
1.	Audit Check list 1: List of documents for understanding the IT system of the auditee.	3
2.	Audit Check list 2: Criticality Assessment tool	5
3.	Audit Check list 3: Collection of specific information on IT Systems	10
4.	Audit Check list 4: Risk Assessment	15
5	Audit Checklist 5: General Controls	23
6	Audit Check list 6: Input Controls	32
7	Audit Check list 7: Processing Controls	35
8	Audit Checklist 8: Output Controls	38
9	Audit Check list 9: IT Security	40
10	Application of CAATs	53

*Audit Check list 1: List of documents for understanding the system*

The commencement of any audit is with the review of the background of the organization to understand its activities and the impact of IT on these activities. This plays important role even in making a criticality assessment. Along with the nature of organization, the audit party would be specifically interested in the background of IT systems in use in the organization. The following illustrative list of documents can be collected for understanding the system.

<b>No.</b>	<b>List of documents</b>
1.	Brief background of the organization
2.	Organisational chart of the entity with details of reporting responsibilities
3.	Personnel policy
4.	Regulations and laws that affect the organisation (for example, Income Tax Act, Company Law etc.)
5.	List of applications and their details
6.	Network and application architecture, including client-server architecture
7.	Organisational structure of the IT department with job descriptions
8.	IT department's responsibilities with reference to the specific application
9.	Business case for the system
10.	Cost associated with the system
11.	Project management reports
12.	Details of hardware
13.	Details of software (including whether developed in-house etc.)
14.	Database details
15.	Data Flow Diagram, Data Dictionary, Table listings
16.	If it is an RDBMS, details of relationships between the tables and database triggers
17.	Details of interfaces with other systems
18.	Systems manual, User manual and Operations manual
19.	Performance analysis reports
20.	List of users with permissions

<b>No.</b>	<b>List of documents</b>
21.	Input output documents
22.	Test data and test results
23.	Security set up for the system
24.	Previous audit reports
25.	Internal audit reports
26.	User feed back about the system
27.	Peer review reports

*Audit Checklist 2: Criticality Assessment tool*

Multiple IT systems may be in use in an organization. The SAI may not be interested in auditing all the IT applications in the government or a particular organization. Further, some applications may be mission critical applications with lapses having far reaching consequences (eg: eSeva or eCops in Andhra Pradesh) where the SAI may prefer to adopt a vigorous framework like CoBIT in conducting the audit. The SAI may not be interested in a comprehensive audit of a simple MIS in a non-critical department where the information generated by MIS is itself not being used by the organization in decision-making. The nature, extent, scope and rigour of the IT audit and the resources committed for the job are dependent upon the subjective assessment of the risk parameters or in other words, criticality of the application. In order to bring some objectivity into the process, though subjectivity cannot in total be avoided, the following criticality assessment tool may be used to categorise the applications based on criticality.

**IT System Risk Assessment Mode** (*figures in parentheses depict the points to be given for that parameter*)

	<b>Name of the Office:</b>		
	Preliminary Information		
A.	Name of the Entity		
B.	Nature of the Entity	Headquarters	
		Regional Office	
		Branch Office	
		Unit Office	
		All of the above	
C.	Name of the System		
D.	Short Description of the System		

**Questions**

<b>1</b>	<b>Does the system relate to any of the following</b>		
	<b>Business Critical Operations</b> For example, Airline/Railway reservations, trading operations, telecom, banking operations, bill generation, on-line bill payment, manufacturing and processing etc.	(30)	
	<b>Name of the Office:</b>		
	Preliminary Information		
	<b>Support Functions</b>	(25)	

	For example, Payroll, Inventory, Financial Accounting, Procurement, Marketing etc.		
	<b>E-Governance</b>	(30)	
<b>2</b>	<b>Investment made in the System</b>		
	Less than Rs.5 lakh	(5)	
	More than Rs.5 lakh less than Rs.25 lakh	(10)	
	More than Rs.25 lakh less than Rs. 50 lakh	(15)	
	More than Rs. 50 lakh less than Rs. 1 crore	(25)	
	More than Rs. 1 crore	(30)	
<b>3</b>	<b>General state of computerization in the entity. The entity has computerized</b>		
	Most of the Business processes	(30)	
	Most of the Accounting and Financial Processes	(25)	
	No business process	(0)	
<b>4</b>	<b>Number of PCs/Desktops used for the system</b>		
	More than 100	(30)	
	More than 50, less than 100	(25)	
	More than 20, less than 50	(15)	
	More than 10 less than 20	(10)	
	Less than 10	(5)	
<b>5</b>	<b>Is the system on the network?</b>		
	Yes		
	No		
	<b>If the system is on the network, is it connected to</b>		
	Internal LAN and/or on intranet?	(20)	
	WAN and MAN and/or on extranet?	(25)	
	Web based /public domain?	(30)	
<b>6</b>	<b>The system is functioning at</b>		
	Only one location	(10)	
	More than one, less than 5 locations	(20)	
	<b>Name of the Office:</b>		
	Preliminary Information		
	More than 5 locations	(30)	

	Is proposed to be expanded in more than one location	(25)	
<b>7</b>	<b>The entity is dependant on the system in as much as</b>		
	Outputs are used for business critical operations /revenue generation	(30)	
	Outputs are manually checked <u>before</u> making payments/raising bills	(10)	
	Outputs are used to prepare Financial Statements	(15)	
	Outputs are not used at all for payment/revenue purposes	(0)	
<b>8</b>	<b>Even though the system does not deal with financial functions, it processes data of public interest. The nature of data is such that, wrong data may lead to :</b>		
	Failure of business	(30)	
	Erosion of credibility of the Organization	(15)	
	Financial loss to the entity	(25)	
	None of the above	(0)	
<b>9</b>	<b>Do the public have access to such data either through web or any other means?</b>		
	Yes, Public can view the data in a dynamic manner	(15)	
	No, Public cannot view the data	(0)	
	Public can transact on-line	(30)	
<b>10</b>	<b>Does the System make use of direct links to third parties e.g. EDI</b>		
	Yes	(20)	
	No	(0)	
<b>11</b>	<b>Does the Organization have dedicated IT Staff</b>		
	Nil	(0)	
	Less than 10	(10)	
	More than 10, less than 30	(20)	
	More than 30, less than 70	(25)	
	More than 70	(30)	
<b>12</b>	<b>Approximately how many persons can be termed as the end-users of the system?</b>		
	<b>Name of the Office:</b>		
	Preliminary Information		
	Less than 5	(0)	

	More than 5, less than 25	(10)	
	More than 25, less than 70	(20)	
	More than 70, less than 150	(25)	
	More than 150	(30)	
<b>13</b>	<b>The system is in operation for</b>		
	More than 10 years	(5)	
	Less than 10 years but more than 5 years	(10)	
	Less than 5 years but more than 2 years	(20)	
	Less than 2 years	(20)	
<b>14</b>	<b>The system is based on</b>		
	Batch Processing	(10)	
	On Line Transaction Processing	(25)	
<b>15</b>	<b>Are there formal change management procedures?</b>		
	<b>Yes</b>	(0)	
	<b>No</b>	(20)	
	<b>How often changes are made to the applications</b>		
	More than 5 times in a year	(30)	
	Less than 5 times in a year more than twice in a year	(20)	
	Less than twice in a year	(10)	
	Not even once in a year	(5)	
<b>16</b>	<b>Does the entity have a documented and approved security policy?</b>		
	Yes	(5)	
	No	(20)	
<b>17</b>	<b>Does the entity use any security software?</b>		
	Yes	(5)	
	No	(20)	
<b>18</b>	<b>Does the entity have a Systems Security Officer?</b>		
	Yes	(5)	
	No	(10)	
	<b>Name of the Office:</b>		
	Preliminary Information		
<b>19</b>	<b>Does the entity have a documented and approved</b>		

	<b>Disaster Recovery Plan?</b>		
	Yes	(0)	
	No	(20)	
<b>20</b>	<b>Volume of data in the system( including off line data) is approximately</b>		
	More than 10 GB	(25)	
	More than 2 GB less than 10 GB	(15)	
	Less than 2 GB	(10)	
	Less than 1 GB	(5)	
	<b>Total Score</b>		

As per the IT system risk assessment tool given above, the points scored are graded below:

<b>Points scored as per risk assessment tool</b>	<b>Classification of risk</b>
Less than 150	Low
Between 150 and 300	Medium
More than 300	High



*Audit Check list 3: Collection of specific information on IT Systems*

The Audit management may require to collect some specific information on the IT systems. The following questionnaires may be used to collect the information at the time of conduct of audit. While some of the information that is collected in Audit Check List 1 may overlap with the information collected in this questionnaire, the current questionnaire will work as a basic tool of audit documentation also. This becomes the reference point for overall comprehension of the system at all stages of the field audit procedures.

*General instructions for collecting information:*

- ✓ There are three Forms to be filled.
- ✓ For item at Sl. No. 3, the name of IT Application (e.g. Passenger Reservation System i.e. PRS in Railways) should be filled in.
- ✓ For item at Sl. No. 4, the name of senior most person should figure in case aggregated data is compiled from more than one location/agency.
- ✓ If the IT system is still under development, information in questionnaire from *Sl. No. 12 to 19 may not be furnished*. In that case Form 3 may be filled and if procurement of H/W for IT system under development has been done, then Form 2 may also be filled.

**Form 1**

1. Name of the auditee organisation:	
2. Date on which information collected :	
3. Name of the IT Application and broad functional areas covered by the IT Application:	
4. Department Head of the Auditee Organisation:	
Name:	
Phone No:	
Email:	
5. Department Head of the Auditee Organisation:	
Name:	
Phone No:	
Email:	

<p>6. Information Systems in-charge:</p> <p style="padding-left: 40px;">Name:</p> <p style="padding-left: 40px;">Phone No:</p> <p style="padding-left: 40px;">Email:</p>	
<p>7. What is (are) the location(s) of the IT system installation(s)?</p>	
<p>8. State the category of IT system architecture:</p>	<p>A. Mainframe based <input type="checkbox"/></p> <p style="padding-left: 20px;">Minicomputer based <input type="checkbox"/></p> <p style="padding-left: 20px;">PC based <input type="checkbox"/></p> <p style="padding-left: 20px;">Others (pl specify)</p> <hr/> <p>B. File server system <input type="checkbox"/></p> <p>Client server system <input type="checkbox"/></p> <p>Distributed processing system <input type="checkbox"/></p> <p>Webbased/EDI <input type="checkbox"/></p> <p>Others (pl specify)</p>
<p>9. State the category of IT application. (Please indicate the choice(s) applicable):</p>	<p>Accounting system <input type="checkbox"/></p> <p>Financial management system <input type="checkbox"/></p> <p>Inventory/Stock Management <input type="checkbox"/></p> <p>Decision support system/MIS <input type="checkbox"/></p> <p>Manufacturing/Engineering <input type="checkbox"/></p> <p>Payroll <input type="checkbox"/></p> <p>Personnel and Administration <input type="checkbox"/></p> <p style="padding-left: 40px;">Marketing <input type="checkbox"/></p> <p style="padding-left: 40px;">Sales <input type="checkbox"/></p> <p style="padding-left: 40px;">e-Governance <input type="checkbox"/></p> <p style="padding-left: 40px;">R&amp;D <input type="checkbox"/></p> <p style="padding-left: 40px;">ERP <input type="checkbox"/></p> <p style="padding-left: 40px;">Others (Please specify) <input type="checkbox"/></p>
<p>10. Whether the above IT application has got a bearing on the financial and accounting aspects of the organisation?</p>	<p>Yes <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>

11. Software used (the Version may also be specified):	
Operating system(s)	
Network software	
Communication Software	
DBMS / RDBMS	
Front end tool	
Programming Language(s)	
Bespoke (Vendor developed)	
Utility Software	
Any other	
12. Is the IT system a mission critical system or an essential system?	Mission critical system <sup>β</sup> <input type="checkbox"/>
	Essential system <sup>γ</sup> <input type="checkbox"/>
13. Has the application system been developed in house or by outsourcing?	In house <input type="checkbox"/>
	Outsource <input type="checkbox"/>
14. In case of outsourcing, specify the name of agency and the contracted amount:	
15. When was the system made operational?	<b>MM</b> <input type="text"/>
	<b>YYYY</b> <input type="text"/>
16. What is the total investment on the IT system project? Indicate the amount in lakhs of rupees against each item <sup>α</sup> :	
	<b>Rupees in lakhs</b>
Hardware items	
Proprietary software	
Application System development cost	
Manpower training cost	
Maintenance of the all components (recurring)	
17. Number of persons engaged for operation of the system?	01 – 10 <input type="checkbox"/>
	11 – 25 <input type="checkbox"/>
	26 – 50 <input type="checkbox"/>
	51 – 100 <input type="checkbox"/>
	> 100 <input type="checkbox"/>
18. What is the average volume of transactional data generated on a monthly basis in terms of	

<sup>β</sup> A mission critical system is an IT system which directly impact the primary function of the organisation e.g. Passenger Reservation System in Indian Railways or eSeva in AP.

<sup>γ</sup> An essential system is an IT system the loss of which causes disruption of some service without disrupting primary services eg: payroll package in police department.

<sup>α</sup> If exact figures are not readily available, approximate figures may be provided.

*IT Audit Manual*

storage space?	
19. Does the system documentation provide for an audit trail of all transaction processed and maintained?	Yes <input type="checkbox"/> No <input type="checkbox"/>
20. Are the manuals as indicated available?	
a. Users documentation manual	Yes <input type="checkbox"/> No <input type="checkbox"/>
b. Systems and programming documentation manual	Yes <input type="checkbox"/> No <input type="checkbox"/>
21. Is there any system in place to make modifications to the application being used on a regular basis to support the function?	Yes <input type="checkbox"/> No <input type="checkbox"/>
22. Does the organisation transmit/receive data to/from other organisations:	Receive <input type="checkbox"/> Transmit <input type="checkbox"/> No <input type="checkbox"/>

**Form 2**

23. Details of all Hardware items including the number of terminals etc. employed:  _____ _____ _____ _____
24. Details of networking hardware employed:  _____ _____ _____
25. Are more than one IT Application(s) running on the same Hardware? If Yes, specify the name(s) of such IT Application(s) apart from the application as indicated at Sl. No. 2.  _____ _____ _____ _____

**Form 3 (For Systems Under Development)**

26. What is the current status of development of IT system if it is still under development? (Tick the appropriate box indicating the current stage of development of IT Application)	Feasibility study stage <input type="checkbox"/> User requirement <input type="checkbox"/> Specification stage <input type="checkbox"/> Design stage <input type="checkbox"/> Development stage <input type="checkbox"/> Testing stage <input type="checkbox"/> Parallel run (if any) <input type="checkbox"/> Implementation stage <input type="checkbox"/>
27. What is the projected cost for the IT system? (Rupees in Lakhs)	Rs. _____ lakhs
28. What is the target date for completion?	_____ (MM/YY)

*Audit Checklist 4: Checklist for Risk Assessment*

The field audit procedures including the types of tests to be undertaking depends on the risk assessment undertaken at the beginning of the audit and the risk perceptions modified at various points of time. The following checklist gives an illustrative checklist of questions to be asked regarding various aspects of IT systems in order to form an opinion about the risk levels. ***These checklists may have to be modified by the auditor based on an understanding of the organisation and the application to be audited.***

No.	Item	Response	
		Yes	No
	<b>Management &amp; Organisation</b>		
1	Is there a strategic IT plan for the organization based on business needs?		
2	Is there a steering committee with well defined roles and responsibilities?		
3	Does the IT department have clear cut and well defined goals and targets?		
4	Is there a system of reporting to top management and review in vogue?		
5	Is there a separation of duties and well defined job characteristics in the IT Department?		
6	Does management provide appropriate direction on end user computing?		
7	Are there appropriate policies and procedures in relation to retention of electronic records?		
8	Where the organisation uses third parties to process data, does it have appropriate procedures in place to address associated risks?		
9	Are there procedures to update strategic IT plan?		
	<b>Personnel policy</b>		
10	Whether criteria are used for recruiting and selecting personnel?		
11	Whether a training needs analysis is done at periodical intervals?		
12	Whether training programmes are periodically held to update knowledge?		
13	Whether organisation's security clearance process is adequate?		
14	Whether employees are evaluated based on a standard set of competency profiles for the position and evaluations are held on a periodic basis?		

No.	Item	Response	
		Yes	No
15	Whether responsibilities and duties are clearly identified?		
16	Whether backup staff is available in case of absenteeism?		
17	Whether there is a rotation of staff policy in key areas where uninterrupted functioning is essential		
	<b>Security</b>		
18	Is there a strategic security plan in place providing centralised direction and control over information system security?		
19	Is there a centralised security organisation responsible for ensuring only appropriate access to system resources?		
20	Is there a data classification schema in place?		
21	Is there a user security profile system in place to determine access on a "need to know basis"?		
22	Is there an employee indoctrination/training system in place that includes security awareness, ownership responsibility and virus protection requirements?		
23	Whether cryptographic modules and key maintenance procedures exist, are administered centrally and are used for all external access and transmission activity?		
24	Whether preventative and detective control measures have been established by management with respect to computer viruses?		
25	Whether change control over security software is formal and consistent with normal standards of system development and maintenance?		
26	Whether password policy exists		
27	Whether access to the VoiceMail service and the PBX system are controlled with the same physical and logical controls as for computer systems?		
28	Whether access to security data such as security management, sensitive transaction data, passwords and cryptographic keys is limited to a need to know basis?		
	<b>Physical &amp; Logical access</b>		
29	Whether facility access is limited to least number of people?		
30	Whether "Key" and "including ongoing card reader" management procedures and practices are adequate, update and review on a least-access-needed basis?		
31	Whether access and authorisation policies on entering/leaving, escort, registration, temporary required passes, surveillance cameras as appropriate to all and especially sensitive areas are adequate?		
32	Is there a periodic and ongoing review of access profiles, including managerial review?		

No.	Item	Response	
		Yes	No
33	Whether security and access control measures include portable and/or off-site used information devices?		
34	Whether review occurs of visitor registration, pass assignment, escort, person responsible for visitor log book to ensure both check in and out occurs and receptionist's understanding of security procedures?		
35	Is there a system of reviewing fire, weather, electrical warning and alarm procedures and expected response scenarios for various levels of environmental emergencies?		
36	Is there a system of reviewing air conditioning, ventilation, humidity control and expected response scenarios for various loss or unanticipated extremes?		
37	Whether health, safety and environmental regulations are being complied with?		
38	Whether physical security is addressed in the continuity plan?		
39	Whether specific existence of alternative infrastructure items necessary to implement security: <ul style="list-style-type: none"> <li>• uninterruptible power source (UPS)</li> <li>• alternative or rerouting of telecommunications lines</li> <li>• alternative water, gas, air conditioning, humidity resources</li> </ul>		
40	Are there procedures to update physical and logical access procedures?		
	<b>Business Continuity &amp; Disaster Recovery</b>		
41	Have the business critical systems been identified?		
42	Has an appropriate business continuity plan been developed, documented and approved?		
43	Whether regular review and update of the plan has been carried out?		
44	Are back up copies of data files and programs taken regularly?		
45	Are the documents of the system and disaster recovery plan appropriately backed up?		
46	Are back up copies held in secure locations both locally and remote from the computer site?		
47	Are the back-up and recovery procedures appropriately tested?		
48	Are the business systems and operations effectively designed to minimize disruption?		
49	Are there procedures to update business continuity and disaster recovery plan?		

No.	Item	Response	
		Yes	No
	<b>Hardware</b>		
50	Is there an organization policy for upgrading the hardware based on technology changes?		
51	Is there an effective preventive maintenance program in place for all significant equipment?		
52	Is equipment downtime kept within reasonable limits (<5%)		
53	Is a reasonable effort made to acquire data centre and networking hardware that is compatible with the existing environment?		
54	Is anyone in the IT organization responsible for identifying potentially unnecessary equipment and taking appropriate action?		
55	Is a formal inventory of all IT hardware available?		
56	Are there procedures to update documentation whenever changes made in the hardware?		
	<b>Software</b>		
57	Is the software used covered by adequate licences?		
58	Is the source code available and if so, accessible at what level?		
59	Is there a system of recording changes to the applications?		
60	Are these changes properly authorized?		
61	Whether emergency change procedures are addressed in operation manuals?		
62	Whether proper testing was carried out and results recorded before final implementation of application?		
63	Is there an exception reporting system in place?		
64	In the case of bought out software are there agreements in place for maintenance and service?		
65	Is there a system of obtaining user feed back and reporting action taken thereon to management?		
66	Is the application design documented?		
67	Whether the programs are documented?		
68	Is the testing methodology documented?		
69	Whether operations procedures are documented?		

No.	Item	Response	
		Yes	No
70	Whether user manuals are available?		
71	Do manuals include procedures for handling exceptions?		
72	Are there procedures to update documentation when an application changes?		
	<b>Data Management</b>		
73	Whether for data preparation the following exist: <ul style="list-style-type: none"> <li>• data preparation procedures ensure completeness, accuracy and validity</li> <li>• authorisation procedures for all source documents</li> <li>• separation of duties between origination, approval and conversion of source documents into data</li> <li>• periodic review of source documents for proper completion and approvals occurs</li> <li>• source document retention is sufficiently long to allow reconstruction in the event of loss, availability for review and audit, litigation inquiries or regulatory requirements</li> </ul>		
74	Whether for data input whether the following exist: <ul style="list-style-type: none"> <li>• appropriate source document routing for approval prior to entry</li> <li>• proper separation of duties among submission, approval, authorisation and data entry functions</li> <li>• audit trail to identify source of input</li> <li>• routine verification or edit checks of input data as close to the point of origination as possible</li> <li>• appropriate handling of erroneously input data</li> <li>• clearly assign responsibility for enforcing proper authorisation over data</li> </ul>		
75	For data processing: Whether programmes contain error prevention, detection, correction routines		
76	Whether error handling procedures include: <ul style="list-style-type: none"> <li>• correction and resubmission of errors must be approved</li> <li>• individual responsibility for suspense files is defined</li> <li>• suspense files generate reports for non-resolved errors</li> <li>• suspense file prioritization scheme is available based on age and type</li> </ul>		

No.	Item	Response	
		Yes	No
77	Whether logs of programmes executed and transactions processed/rejected for audit trail exist?		
78	Whether there is a control group for monitoring entry activity and investigating non-standard events, along with balancing of record counts and control totals for all data processed?		
79	Whether written procedures exist for correcting and resubmitting data in error including a non-disruptive solution to reprocessing?		
80	Whether resubmitted transactions are processed exactly as originally processed?		
81	Whether responsibility for error correction resides with original submitting function?		
82	Whether Artificial Intelligence systems are placed in an interactive control framework with human operators to ensure that vital decisions are approved?		
83	Whether for output, interfacing, and distribution whether the following exist: <ul style="list-style-type: none"> <li>• Access to output is restricted physically and logically to authorised people</li> <li>• Ongoing review of need for outputs is occurring</li> <li>• Audit trails to facilitate the tracing of transaction processing and the reconciliation of disrupted data</li> <li>• Process and responsibility of output disposal is clearly defined</li> <li>• All input and output media is stored in off-site location in event of later need</li> </ul>		
84	Whether for media library the following exist: <ul style="list-style-type: none"> <li>• Contents of media library are systematically inventoried</li> <li>• Housekeeping procedures exist to protect media library contents</li> <li>• Responsibilities for media library management have been assigned to specific members of IT staff</li> <li>• Media back-ups and restoration strategy exists</li> <li>• Media back-ups are taken in accordance with the defined back-up strategy and usability of back-ups is regularly verified</li> <li>• Media back-ups are securely stored and storage sites periodically reviewed regarding physical access</li> </ul>		

No.	Item	Response	
		Yes	No
	<ul style="list-style-type: none"> <li>• security and security of data files and other items</li> <li>• Retention periods and storage terms are defined for documents, data, programmes, reports and messages (incoming and outgoing) as well as the data (keys, certificates) used for their encryption and authentication</li> </ul> <p>Adequate procedures are in place regarding the archival of information (data and programmes) in line with legal and business requirements and enforcing accountability and reproducibility</p>		
85	<p>Whether for information authentication and integrity the following exist:</p> <ul style="list-style-type: none"> <li>• The integrity of the data files is checked periodically</li> <li>• Requests received from outside the organisation, via telephone or Voicemail, are verified by call-back or other means of authentication</li> <li>• Electronic signature or certification is used to verify the integrity and authenticity of incoming electronic documents</li> </ul>		
	<b>Internal Audit</b>		
86	Does the organization have Internal audit section in the area of IT system?		
87	Does the organization utilize IT auditors in the internal audit functions?		
88	Are the IT auditors trained to effectively use IT audit tools and techniques?		
89	Are highly technical IT audits only done by internal auditors with comparable skills?		
90	Does the internal IT audit staff provide technical support for the financial and general auditors?		
91	Is the IT audit function subject to periodic peer reviews?		
92	Does the IT audit include an assessment of compliance with organizations policies, procedures and standards?		
93	Does the internal audit cover an analysis of all the areas processed by the applications?		
94	Does the internal audit include an analysis of internal controls?		

No.	Item	Response	
		Yes	No
95	Does the internal audit include an assessment of the application documentation?		
96	Does the internal audit include an assessment as to whether transactions are completely and correctly processed on a timely basis?		
97	Are the internal audit reports seen by top management?		
98	Has action being taken on the basis of recommendations in the internal audit reports?		
99	Is the periodicity of internal audit reports adequate?		
100	Is there a system of training and updation of skills for internal IT auditors?		
101	Whether internal audit has been involved in system development?		

Here it is important to reiterate that negative response to any of the question is to be weighed in with two factors:

- The criticality of the application for the organization and
- The role played by the organization in the larger scheme of things.

For example poor physical access controls would be of great relevance in an office automation system in ministry of defence, home affairs etc. Similarly Back up procedures would be more important in financial institutions. The Auditor has to exercise his/her judgement in deciding the risk profile of the organization or the application to be audited.

*Audit Checklist 5: General Controls*

General Controls are the controls applicable for entire IT System. They can be computer based controls or non-computer based controls. One of the popular premises of IT Audit is that examining the application controls is of no consequence unless the general controls are strong. IT Audit in SAI, India includes examination of the general controls and application controls. While examining controls, it is important for the audit party not to jump to audit conclusions based on the isolated instances of weak controls. The controls have been viewed in relation to the impact on the efficiency, security or effectiveness of the system. Further the costs of controls have to be justified based on the benefits derived. Technology is a tool that can provide any extent of granularity of control and security. However, higher costs of usually associated with stronger controls and audit has to examine the risk of absence or weakness of a control compared with its cost. Another important caution for the audit party is that even if a critical control is absent, the party has to look for compensating controls. The weakness in one control may be commensurate with a stronger control elsewhere.

<b>Organisational and Management Controls</b>		<b>KD reference</b>
1.	<p>Considering whether IT or business enterprise policies and procedures address a structured planning approach and a methodology is in place to formulate and modify the plans and at a minimum, they cover:</p> <ul style="list-style-type: none"> <li>• organisation mission and goals</li> <li>• IT initiatives to support the organisation mission and goals</li> <li>• opportunities for IT initiatives</li> <li>• feasibility studies of IT initiatives</li> <li>• risk assessments of IT initiatives</li> <li>• optimal investment of current and future IT investments</li> <li>• re-engineering of IT initiatives to reflect changes in the enterprise’s mission and goals</li> <li>• evaluation of the alternative strategies for data applications, technology and organisation</li> </ul>	
2.	<p>How appropriate is the audited body’s IT strategic plan?</p> <ul style="list-style-type: none"> <li>• Has it been documented?</li> <li>• Has it been approved?</li> <li>• Is it kept up to date?</li> <li>• Does it cover the financial information systems?</li> <li>• Is staff informed of the issues?</li> </ul>	

<b>Organisational and Management Controls</b>		<b>KD reference</b>
3.	Does the strategic plan identify target dates, resources, and personnel needed to accomplish the plan?	
4.	Are there procedures for monitoring its implementation?	
5.	Are current IT activities consistent with the plan?	
6.	How does senior management maintain an appropriate level of interest in the audited body's IT functions? (e.g. through an IT steering committee.)	
7.	Determine if committees (e.g. IT steering committee) review, approve, and report to the Board on: <ul style="list-style-type: none"> <li>• Short and long term information systems plans</li> <li>• IT operating standards</li> <li>• Data security policies and procedures</li> <li>• Resource allocation (major hardware/software acquisition and project priorities)</li> <li>• Status of major projects</li> <li>• IT budgets and current operating cost</li> </ul>	
8.	Does the organisation have adequate IT documentation policies? Policies should ensure that documentation is up to date, comprehensive and available to appropriate staff.	
9.	Does the organisation's internal audit function carry out IT reviews of the computerised financial systems?	
10.	Is the organization considering applicable rules and regulations like tax laws, company legislation requirements while forming document retention policies?	
11.	Are policies for recruitment, screening and disciplinary procedures appropriate for the IT environment?	

<b>Organisational and Management Controls</b>		<b>KD reference</b>
12.	Are there procedures in place for updating the skills of end users and trainings arranged regularly?	
13.	Assess whether Training programmes are consistent with the organisation's documented minimum requirements concerning education and general awareness covering security issues	
14.	Are critical jobs rotated periodically?	
15.	Does the organisation have appropriate policies and procedures for ensuring that its IT facilities comply with legal and regulatory requirements?	
16.	Does the audited body receive IT services from external sources? Have appropriate procedures been developed to meet identified risks (e.g. access rights)?	
17.	Is there a separation of duties and well defined job characteristics in the IT projects	
	<b>IT Operational Controls</b>	
18.	Determine if there are adequate standards and procedures for: <ul style="list-style-type: none"> <li>• Systems development</li> <li>• Program change control</li> <li>• Data Centre operations</li> <li>• Data Base administration</li> <li>• Performance monitoring</li> <li>• Capacity planning</li> <li>• Network administration</li> <li>• Information security</li> <li>• Contingency planning/disaster recovery</li> </ul>	
19.	Obtain and review copies of all vendor and consultant contracts, available financial statements and escrow agreements.	
20.	Determine if: <ul style="list-style-type: none"> <li>• Overall systems and program documentation adheres to standards.</li> <li>• Documentation is complete and current.</li> </ul>	

<b>Organisational and Management Controls</b>		<b>KD reference</b>
21.	Determine if the security procedures cover: <ul style="list-style-type: none"> <li>• Physical protection of the facility.</li> <li>• Designation and duties of the security officer(s).</li> <li>• Authorised data and program access levels.</li> </ul>	
22.	<ul style="list-style-type: none"> <li>• Requirements for password creation and change procedures.</li> <li>• Requirements for access via terminals, modems or computer system (LAN) connection.</li> <li>• Monitoring and follow-up of security violations.</li> </ul>	
23.	Has management established security requirements, and penal/ corrective action in case of failure, as part of contracts with third-party service providers?	
24.	<p>A range of controls is required where an organisation uses computer networks. The typical controls would include:</p> <p><b>Separation of duties between operators and network administrators;</b></p> <p><b>Establishment of responsibility for procedures and management of remote equipment;</b></p> <p><b>Monitoring of network availability and performance. There should be reports and utilities to measure system response time and down time; and</b></p> <p><b>Establishment and monitoring of security controls specific to computer network.</b></p> <p><b>Verify if the above mentioned network controls are in place</b></p>	
25.	Determine whether procedures are in place to update the security policy. Ensure updates to the policy and procedures are distributed to and reviewed by management.	
26.	Determine if an education program has been implemented to promote user awareness about security policies and procedures.	

<b>Organisational and Management Controls</b>		<b>KD reference</b>
<b><i>Physical Controls (Access and Environment)</i></b>		
27.	<b>Determine whether there are procedures in place to prevent any unauthorised entry into the IT facilities of the organisation.</b>	
28.	Are there adequate and effective countermeasures relating to physical security against different environmental threats e.g. fire, flood, electrical surges, lightning, etc.?	
<b>Logical Access Controls</b>		
28	Whether passwords are keyed in using nonprinting, nondisplaying, facilities.	
29	Whether security breaches are immediately reported for appropriate action.	
30	Does this report identifies the terminal and displays the date and time of incident.	
31	Does the system have a predetermined number of failure attempts before shutting down which can then only be started by specially authorized personnel.	
32	Is a data-access matrix used to define access levels?	
33	Does the senior management regularly review the adequacy of the data access matrix?	
34.	Whether procedures are in place for issuing, approving and monitoring application access and whether such procedures comply with the policy of “minimum access”.	
35.	How security violations are detected and reported. See the presence or absence of terminal logs.	
36.	Determine that password security is in effect on all applications and assess the adequacy of controls over: <ul style="list-style-type: none"> <li>• Password Change on a regular basis</li> <li>• Suppressing passwords’ display on a terminal.</li> </ul>	
37.	Examine if system access levels are consistent with job functions.	

<b>Organisational and Management Controls</b>		<b>KD reference</b>
38.	Does the security software provides an adequate audit trail to identify the programmer, the programs or utilities used, the files or programs accessed and the nature of the access.	
39.	Are there well-defined procedures for user account management, including clear and effective linkages between user rights and current positions, as well as termination of user rights on cessation of employment etc.?	
40.	If physical or logical separation between the production and test environments is maintained.	
41.	Assess the adequacy of segregation of duties for application programming, systems programming, computer operation, and system security functions.	
42.	Determine that passwords are removed as soon as an individual's employment is terminated to ensure that a terminated employee cannot gain access to the computer files through an outside terminal.	
43.	Have adequate preventive, as well as detective control measures been taken by management with regard to computer viruses at all levels, ranging from high end servers to user desktops and laptops?	
<b><i>Controls over IT Acquisition</i></b>		
44.	•	
45.	Consider whether <ul style="list-style-type: none"> <li>• The IT budgetary process is consistent with the organisation's process</li> <li>• Policies and procedures are in place to ensure the preparation and appropriate approval of an annual IT operating budget which is consistent with the organisation's budget and long- and short-range plans, and the IT long- and short-range plans</li> <li>• The budgetary process is participatory with the management of the IT function's major units contributing in its preparation</li> </ul>	

<b>Organisational and Management Controls</b>		<b>KD reference</b>
	<ul style="list-style-type: none"> <li>• Policies and procedures are in place to regularly monitor actual costs and compare them with the projected costs, and the actual costs are based on the organisation's cost accounting system</li> <li>• Policies and procedures are in place to guarantee that the delivery of services by the IT function is cost justified and in line with industry costs</li> </ul>	
46.	Ensure organisational adherence to a structured approach, comprising all the key acquisition activities and deliverables, timelines and milestones etc.	
47.	Assess whether there is a defined evaluation and selection criteria, to minimize acquisition and project risks.	
48.	Whether compatibility with the organisation's acquisition policies and procedures, including any applicable regulatory guidelines has been ensured in IT acquisition.	
49.	<b>The objectives, scope and requirements of the acquisition should be clearly defined and documented, including any integration issues that need to be addressed.</b>	
<b><i>Program Change Controls</i></b>		
50.	Verify that a methodology is used for initiation and approval of changes.	
51.	If all changes to the system security software are approved by the system security administrator.	
52.	Ensure all changes are applied to a copy of the latest production version of code.	
53.	Whether the change control log ensures all changes shown were resolved?	
54.	Whether the changes to requirements resulted in appropriate changes to development documents, such as technical and operational manual?	
55.	Whether established procedures were there for ensuring executable and source code integrity?	

<b>Organisational and Management Controls</b>		<b>KD reference</b>
56.	Verify that the changed code is tested in a segregated/controlled environment	
57.	Determine to what extent the user is involved in the testing process	
58.	Ensure that a backout process is developed before any change request is implemented	
	Business continuity and disaster recovery controls	
59.	Determine if IT facility has a documented disaster recovery plan.	
60.	Verify that the IT disaster recovery plan supports the goals and priorities found in the corporate business continuity plan.	
61.	<p>Review the IT disaster recovery plan to determine if it:</p> <ul style="list-style-type: none"> <li>• Clearly identifies the management individuals who have authority to declare a disaster.</li> <li>• Clearly defines responsibilities for designated teams or staff members.</li> <li>• Explains actions to be taken in specific emergency situations.</li> <li>• Allows for remote storage of emergency procedures manuals.</li> <li>• Defines the conditions under which the backup site would be used.</li> <li>• Has a procedure in place for notifying the backup site.</li> <li>• Has a procedure for notifying employees.</li> <li>• Establishes processing priorities to be followed.</li> <li>• Provides for reserve supplies.</li> </ul>	
62.	Determine if all critical resources are covered by the plan.	
63.	Determine if all master files and transaction files are backed up adequately to facilitate recovery.	
64.	Determine if the IT disaster recovery plan is tested periodically, including critical applications and services	

<b>Organisational and Management Controls</b>		<b>KD reference</b>
65.	Determine if the tests include: <ul style="list-style-type: none"><li>• Setting goals in advance.</li><li>• Realistic conditions and activity volumes.</li><li>• Use of actual backup system and data files from</li></ul>	
66.	67. off-site storage. 68. Participation and review by internal audit. 69. A post-test analysis report and review process that includes a comparison of test results to the original goals. 70. Development of a corrective action plan for all problems encountered.  Determine if several user departments have been involved in testing at the same time to uncover potential conflicts.	

*Audit Checklist 6: Input Controls*

Input controls are the application controls which seeks to minimize the risk of incorrect data entry by making validation checks, duplicate checks and other related controls. These provide the earliest opportunity to detect and correct possible mistakes. The following checklist can be used to examine the input controls:

<b>Sl No</b>	<b>Item</b>	<b>KD reference</b>
1.	Examine the methods of data entry and conversion. Are the methods well documented?	
2.	Is there adequate segregation of duties commensurate with the size of the organization and nature of functions?	
3.	Does one individual perform more than one function with reference to Data origination, data input, data processing or data distribution? If so does compensating controls exist to protect against the risks of clubbing functions?	
4.	Is there a system of control group with responsibility for data conversion and entry of all source documents received from user departments?	
5.	Are the turnaround documents returned to user department by control group ensuring that no documents are added or lost?	
6.	Is there a system of independent control group reconciling the record count with record counts of user department control groups?	
7.	Are any discrepancies in control group totals noticed? If so are they reconciled?	
8.	Does the Data Processing group (DP) group maintain a log of all the user departments source documents received and their final disposal?	
9.	Are all the documents accounted for? If so what is the method used?	
10.	Is there a system of scheduling and time planning in the DP department for receipt of data requiring entry and its completion time?	
11.	How is it ensured that all the documents are entered into the system once and only once, thereby preventing duplication?	
12.	Is there a system of documents being signed or marked to prevent reuse of data?	
13.	Does the DP control group receive all turnaround documents to ensure that no documents are added or lost during data entry?	
14.	Is there segregation of duties to ensure that the person keying the data is not also responsible for verification of document	
15.	Does the system incorporate necessary data validation and editing errors at the earliest instant to ensure that application rejects any transaction before its entry into the system?	

SI No	Item	KD reference
16.	Are there essential input validations with reference to codes, fields, characters, transactions, calculations, logic, units, reasonableness, sequence etc?	
17.	Is there a system of special routines used that automatically validates and edit input transaction dates against predetermined cut-off dates?	
18.	Is there a possibility of date entry or other personnel bypassing or overriding the data validation and edit controls?	
19.	If so, is the authority to override restricted to only supervisory staff and to limited number of approved situations	
20.	If the system of override exists, each instance of system override should be logged and reviewed for appropriateness	
21.	If data is rejected by application, are there documented procedures in place to identify, correct and reprocess such data?	
22.	Is there a system of clear and compact error messages communicating the problems so that immediate corrective action can be taken for each type of error	
23.	Does the system provide for error messages for every type of error (field level or transaction level) not meeting the edit validation	
24.	How are rejected items recorded? Are they automatically written in a suspense file?	
25.	Does the automated suspense file include codes indicating error types, date and time of entry and identify the person entering data?	
26.	How are the automated suspense files used in correction and re-entry of transactions rejected by the application?	
27.	Does the automated suspense file provide information and analysis on the level of transaction errors and status of uncorrected transactions for management review?	
28.	Does management, based on the analysis, when error levels become too high take necessary correction?	
29.	Is there a system of escalation of reports to higher levels if the conditions deteriorate?	
30.	In case of keying and authorizing passwords or secret authorizing codes, does the system ensure use of non-displaying and nonprinting facilities to ensure that there is no compromise?	
31.	(i) In case of attempted unauthorized terminal access, does the necessary alert and report get produced automatically?  (ii) If so, does the report identify the location of device used for unauthorized access attempt, date and time of violation, number of attempts and identification of the operator?	
32.	In case of a predetermined unauthorized access attempts, does the system provide for terminal lockup to prevent compromise?	

<b>Sl No</b>	<b>Item</b>	<b>KD reference</b>
33.	In case of terminal lockup, does the system automatically shut down terminal and can be opened only by authorized DP department supervisors after scrutiny?	
34.	Does the organization provide for a data access matrix defining the access rights and limiting the access based on user identification, authentication and authorization?	
35.	Is there a limit on online system users restricting them to certain types of transactions only?	
36.	Is there adequate limitation and control on the access to master commands controlling operations to limited authorized supervisory DP personnel?	
37.	Is there a system of senior management review of terminal authority levels for adequacy and suitability?	
38.	What is the password policy of the organization? Is there a system of forced periodic password change?	
39.	In case of a real or purported security violation, are passwords changed?	
40.	When an individual leaves the job or changes the function, are the passwords deleted? Is the user account used by successor with same user name?	
41.	Does the terminal hardware have features of in-built terminal identification and authorization and messages date and time stamped?	
42.	What are the contents of message header? Does it include the essentials of message number, terminal and user identification, date and time, transaction code etc?	
43.	Do the messages end with a message footer indicating the end of message and end of transmission?	
44.	During data entry can the terminal operator interact with the system	
45.	Does the system prompt at appropriate instances to facilitate data entry and minimize errors (use of computer – aided instructions)?	

*Audit Checklist 7: Processing Controls*

Processing Controls are the application controls that ensure that complete and correct processing of input. They also ensure that incorrect transactions are not processed. The following check list may be used in examining and evaluating processing controls:

<b>Sl No</b>	<b>Item</b>	<b>KD reference</b>
1.	Do documented procedures exist explaining the methods for proper processing of each application program?	
2.	Is there adequate segregation of duties in respect of processing commensurate with the size of the organization and nature of functions?	
3.	Does one individual perform more than one function with reference to Data origination, data input, data processing or data distribution? If so does compensating controls exist to protect against the risks of clubbing functions?	
4.	Does an effective system of operator instructions exist including system start-up procedures, backup assignments, emergency procedures, system shutdown procedures, debugging facility, error message instructions etc?	
5.	Examine the Program Run Books for their effectiveness based on setup procedures, input source and data formats, lights out operations, halt conditions, restart and checkpoint facilities, output data and formats, system flow charts etc?	
6.	Does the console depict the history log?	
7.	Does the history log include hardware and software failure errors, processing halts, abnormal termination of jobs, operator interventions, unusual occurrences etc?	
8.	Is the history log reviewed for identification of problems and corrective action?	
9.	Is there a system of scheduling in position application-wise indicating the time when application programmes should be run and completed?	
10.	Examine the system of control group independently controlling data processing using batch counts, record counts, control totals, logs of input/output etc	
11.	Is there a system of unique identifier or transaction code present directing the transaction to the proper application programme for processing?	
12.	Does the computer programme logic have in-built standardized default options?	
13.	Are version control procedures in place ensuring the processing on the proper version of file?	
14.	Examine the system of Application file process to ensure that master and transaction files are properly and completely processed.	

<b>Sl No</b>	<b>Item</b>	<b>KD reference</b>
15.	Are input counts reconciled with output counts to ensure completeness of data processing?	
16.	Examine the reconciliation between sending program output and receiving program input thereby establishing an effective control over processing.	
17.	Examine the stage at which data validation and edit checks are performed so as to ensure the early detection and rejection of incorrect transactions	
18.	Examine the validation checks with reference to codes, characters, fields, transactions, calculations, missing data, logic etc to ensure validity of all data input	
19.	Check the system of LOV (List of Values) contained in a table ensuring their accuracy and integrity	
20.	In case of data rejection, does the organization have a well documented procedure to identify, correct and reprocess data rejected	
21.	Are the error messages clear and short communicating the nature of error for appropriate guidance to user	
22.	Whether Audit trail exists depicting the flow of transaction at every point of processing upto the output stage?	
23.	Is it possible to irrefutably trace the transaction from its destination to its point of origin?	
24.	Is there a system, if required, of protection against concurrent file updates by locking the file / record when an application accesses the same for update purposes?	
25.	Examine the system of date and time stamping of transactions for log and audit trail purposes	
26.	Examine the log of transactions to include hardware failure messages, processing halts, abnormal termination of jobs, software failure messages, error messages etc	
27.	Examine the role of control group in investigating and correcting any terminal problems that can be resolved at the sources; investigating operator interventions; monitoring terminal activity; investigating operator deviations from roles etc	
28.	Check the mechanism of accuracy in master file contents by taking periodic samples	
29.	Examine whether the input transactions have unique transaction identifier facilitating its processing in the proper application	
30.	In case of direct update to files, examine whether a record is created and added to back up file containing a before and after image of the record being updated	
40.	In case of direct update to files, whether transaction history file records transaction's time and date and the unique identifier of the originator of the update	

<b>Sl No</b>	<b>Item</b>	<b>KD reference</b>
41.	Is there a system of supervisory review of all corrections in place before their re-entry	
42.	Does the organization provide for same level of security in processing corrected transactions as in the case of original transactions including supervisory review	
43.	Is the user ultimately responsible for complete and accurate processing of data	

*Audit Checklist 8: Output Controls*

Output controls are the processing controls that ensure that the output is complete, accurate, timely and is correctly distributed. The following checklist can be used for examining and evaluating the output controls in the implementation of an application:

<b>Sl No</b>	<b>Item</b>	<b>KD reference</b>
1.	Examine the balancing and reconciliation of output as established by documented methods.	
2.	Does a control group exist ensuring processing flow as per the schedule	
3.	Whether output is reviewed by a control group for acceptability, accuracy and completeness.	
4.	Examine the system of reconciliation of output batch control totals with input batch control totals before release of reports establishing data integrity	
5.	Examine the reconciliation between input record counts with output record counts by a control group before release of reports	
6.	Are the predetermined output control totals reconciled with pre-determined input control totals by a control group before release of reports ensuring data integrity	
7.	Examine the control group log summarizing the number of application reports generated, number of lines per report, number of pages per report, recipients of each report and number of copies of each report	
8.	Whether output audit trial logs are maintained and periodically reviewed by supervisors to ensure accuracy of output generated	
9.	Examine the system of comparison of transaction log kept by the application with the transaction log at each output device to ensure that all transactions have been processed completely	
10.	Examine the system of forward linkage to trace transaction from its origin to its final output stage	
11.	Examine the system of backward linkage to trace transaction from its output stage to its point of origin (data entry)	
12.	Does the application ensure that each output product contains processing programme name or number; title or description; processing period covered; user name and location; date and time prepared; security classification for product etc	
13.	Examine the system of reconciliation of computer generated batch totals with manually developed batch totals by the control group	
14.	Examine the system of reconciliation of computer generated record counts with manually developed record counts by the control group	

<b>Sl No</b>	<b>Item</b>	<b>KD reference</b>
15.	Is there a mechanism with the control group to ensure completeness and accuracy of all output	
16.	Is the user department responsible for correctness of all output	
17.	Examine whether document methods are in place for proper handling and distribution of output	
18.	Examine the interaction with users to determine the needs of the users and the number of copies of the output required	
19.	Are the recipient name and location printed on the cover sheet of every report thereby preventing its unauthorized access	
20.	Examine the Date Processing control group method of scheduling out processing and distribution of output	
21.	Whether appropriate control exists in respect of production, storage and issue of tapes and other magnetic and digital media	

*Audit Checklist 9: IT Security*

One of the core areas of field audit procedures done by the audit party is the examination and evaluation of the IT Security. The grade and granularity of the IT Security is dependent upon general controls, application controls, security policy of the organization and its risk perception. No questionnaire can provide a comprehensive list of all issues relating to IT Security. The audit team need to use is experience and expertise in understanding the need and evaluation the security concerns and issues. *Points may be common between the Information Security list and that of the risk assessment and Input/Processing/Output checklists. The list should be customised according to the individual characteristics of the applications and the organizations role and objectives of the auditees.*

No	Item	KD Reference
<b>I. SECURITY POLICY</b>		
<i>Information Security Policy: To provide management direction and support for information security.</i>		
1.	Information Security Policy Document	Is there a policy document approved by management, published and communicated, as appropriate, to all employees?
2.	Review and Evaluation	Is the policy reviewed regularly and amended when influences cause a change?
<b>II. ORGANIZATIONAL SECURITY</b>		
<i>Information Security Infrastructure: To manage information security within the organization</i>		
1.	Management Information Security forum	Has a management forum been set up to ensure that clear direction and management support is visible and to promote security through appropriate commitment and resourcing?
2.	Information Security Coordination	Depending On the size of the organization, has a cross-functional forum been set up to co-ordinate the implementation of the ISMS (Information Security Management System)?
3.	Allocation of Information Security Responsibility	Have the responsibilities for the protection of individual assets and for carrying out specific security processes been clearly defined?

No	Item	KD Reference	
4.	Authorization process for Information Processing Facility	Is there a process whereby management must authorize new information processing facilities?	
5.	Specialist Information Security Advice	Is there evidence that in-house or specialist advice on information security has been sought and communicated to all employees as appropriate?	
6.	Cooperation Between Organizations	Where appropriate, is communication maintained with law enforcement agencies, regulatory bodies, information service providers and telecommunications operators?	
7.	Independent review of Information Security	Is there an independent review of the implementation of the information security policy? (This may be in-house).	
8.	Security of Third-Party access	To maintain the security of organizational information processing facilities and information assets accessed by third parties	
9.	Identification of Risk from Third-party Access	Has there been an assessment of the risks associated with third parties having access to facilities and assets? And have appropriate security controls been implemented?	
10.	Security Requirements in third-Party Contract	Is there a formal contract between the organization and the third party? e.g. confidentiality undertaking etc.	
11.	Outsourcing	To maintain the security of information when the responsibility for information processing has been outsourced to other organizations	
12.	Security requirements in outsourcing contracts	Where any outsourcing of the management and control of all or some information systems, networks and/or desk top environments is carried out, are there contracts in place between the organization and the sub-contractor?	
<b>III. ASSET CLASSIFICATION AND CONTROL</b> Accountability of asset: <i>To maintain appropriate protection of organizational Assets</i>			
1.	Inventory of Asset	Is there an inventory maintained of all important assets? (Assets being the information held by the organization)	
2.	Information Classification	To ensure that information assets receive an appropriate level of protection	

No	Item	KD Reference	
3.	Classification guidelines	Have the 'important' assets been classified in some form, that identifies the status/importance of each type of information in terms of risk?	
4.	Information labelling and handling	Have a set of procedures been written describing the labelling and handling of information in accordance with the classification register (or similar format)? (the higher the classification, the greater the controls)	
<p><b>IV. PERSONNEL SECURITY</b></p> <p>Security in job definition &amp; resourcing: <i>To reduce the risks of human error, theft, fraud or misuse of facilities</i></p>			
1.	Including Security in job responsibility	Are security roles described in job descriptions or similar?	
2.	Personnel screening and policy	Are appropriate verification checks carried out on permanent staff at the time of job application?	
3.	Confidentiality agreements	Have all employees signed a confidentiality undertaking?	
4.	Terms & condition of employment	Do contracts/terms of employment include the employee's responsibilities for information security?	
5.	Users training	To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work	
6.	Information security education & training	Is there evidence that all appropriate employees and third parties have received training and updates in security policy and procedures?	
7.	Responding to security incidents & malfunctions	To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents	
8.	Reporting Security incidents	Is there a formal system to allow security incidents to be reported through management channels and in a timely manner?	
9.	Reporting security weakness	Are users of information services required to note and report and observed or suspected security weaknesses and or threats to systems and services?	
10.	Reporting software malfunctions	Is there a procedure for reporting software malfunctions?	

No	Item	KD Reference	
11.	Learning from incidents	Is there a review of incidents and malfunctions to determine the types, frequencies and costs associated with the incidents and malfunctions, to enable preventive actions?	
12.	Disciplinary process	Is there a formal disciplinary procedure in place, to address violations of the policy and procedures by employees?	
<b>V. PHYSICAL &amp; ENVIRONMENTAL SECURITY</b> <i>Secure Area : To prevent unauthorized physical access, damage and interference to business premises and information</i>			
1.	Physical security perimeter	Where appropriate, have security perimeters been established to contain information processing facilities?	
2	Physical entry controls	Are secure areas protected by appropriate entry controls to ensure that only authorized personnel are allowed access?	
3.	Security offices, rooms and facilities	Have secure areas been created to protect offices, rooms and facilities with special security requirements?	
4.	Working in secure area	Where appropriate, have any additional controls and guidelines for working in secure areas, to enhance the security, been established?	
5.	Isolated delivery and loading areas	Are delivery and loading areas isolated from information processing facilities, to avoid unauthorized access?	
6.	Equipment security	To prevent loss, damage or compromise of assets and interruption to business activities	
7.	Equipment siting and protection	Is equipment sited or otherwise protected to reduce the risk from environmental threats and hazards, and opportunities for unauthorized access?	
8.	Power supplies	Is equipment protected from power failures, surges and other anomalies?	
9.	Coding security	Is power and telecommunications cabling protected from interception or damage?	
10.	Equipment maintenance	Is equipment maintained in accordance with manufacturer's instructions and/or documented procedures?	
11.	Security of equipment off – premises	Where equipment is used outside the organization's premises, are security procedures and controls in place?	

No	Item		KD Reference
12.	Secure disposal or re-use of equipment	Before any equipment is disposed of, is there a record that information has been erased?	
13.	General controls	To prevent compromise or theft of information and information processing facilities	
14.	Clear desk and clear screen policy	Does the organization have a clear desk and clear screen policy and is it implemented to reduce risks of unauthorized access?	
15.	Removal of property	When equipment, information or software removed from the organization, is there evidence of authorization?	
<b>VI. COMMUNICATION AND OPERATIONS MANAGEMENT</b> Operational procedure and responsibility: <i>To ensure the correct and secure operation of information processing facilities</i>			
1.	Documented operating procedures	Are documented procedures in place for each of the control objectives selected?	
2.	Operational change contracts	Is there a procedure to control changes to information processing facilities and systems?	
3.	Incidents management procedures	Have incident management responsibilities and procedures been written?	
4.	Segregation of duties	As appropriate, are some duties and areas of responsibilities segregated in order to reduce opportunities for unauthorized modifications or misuse of information or services?	
5.	Separation of developments and operational facilities	Are development and testing facilities separated from operational facilities?	
6.	External facilities management	If sub-contract facilities management services are used, have the risks been identified and evaluated and controls agreed with the sub-contractor via a formal contract?	
7.	System planning and acceptance	To minimize the risk of systems failure	
8.	Capacity Planning	Are reviews (or similar) conducted to evaluate and monitor capacity demands to ensure adequate processing power and storage is available now and for the foreseeable future?	

No	Item	KD Reference	
9.	System acceptance	Has the organization established acceptance criteria for new information systems, upgrades and new versions, and have tests been performed prior to acceptance?	
10.	Protection against malicious software	To protect the integrity of software and information from damage and malicious software	
11	Control against malicious software	Have detection and prevention controls been put in place to protect against malicious software and have appropriate user awareness procedures been implemented?	
12.	House keeping	To maintain the integrity and availability of information processing and communication services	
13.	Information Back-up	Are back-up copies of essential business information and software taken regularly? Look for evidence and records.	
14.	Operator logs	Do operational staff maintain a log of their	
15.	Fault logging	Are faults recorded and corrective actions taken by authorized personnel?	
16.	Network management	To ensure the safeguarding of information in networks and the protection of the supporting infrastructure	
17	Network controls	Are suitable controls in place to achieve and maintain security in networks?	
18.	Media handling & security	To prevent damage to assets and interruptions to business activities	
19.	Management of removable computer media	Is the management of removable computer media, such as tapes, disks, cassettes and printed reports suitably controlled?	
20.	Disposal of media	Is media disposed of securely and safely when no longer required?	
21.	Information handling procedures	Are procedures in place for the handling and storage of information in order to protect it from unauthorized disclosure or misuse?	
22.	Security of system documentation	Is system documentation protected from unauthorized access?	

No	Item		KD Reference
23.	Exchange of information and software	To prevent loss, modification or misuse of information exchanged between organizations	
24.	Information and software exchange agreements	Are agreements in place (may be formal as appropriate) for the electronic or manual exchange of information and software between organizations?	
25.	Security media in transit	When media is transported, is it protected from unauthorized access, misuse or corruption?	
26.	Electronics commerce security	Is electronic commerce protected against fraudulent activity, contract dispute and disclosure or modification of information?	
27.	Security of electronic mail	Is there a policy for the use of e-mail to reduce security risks created by e-mail?	
28	Security of electronic office systems	Are policies and guidelines in place and implemented to control the business and security risks associated with electronic office systems?	
29.	Publicly available system	Is there a formal authorization process before information is made publicly available and is the integrity of such information protected to prevent unauthorized modification?	
30.	Other forms of information exchange	Are procedures and controls in place to protect the exchange of information through the use of voice, fax and video communications facilities?	
<b>VII. ACCESS CONTROL</b>			
Business requirement for access control: <i>To control access to information</i>			
1.	Access control policy	Is there an access control policy and is access restricted in accordance with the policy?	
2.	User Access management	To prevent unauthorized access to information systems	
3.	User registration	Is there a formal user register and de-registration procedure for granting access to all multi-user information systems and services?	
4.	Privilege management	Is the allocation and use of privileges restricted and controlled?	
5.	User password management	Is the allocation of passwords controlled through a formal management process?	
6.	Review of user access rights	Are users' access rights reviewed at regular intervals via a formal process?	

No	Item		KD Reference
7.	User responsibility	To prevent unauthorized user access	
8.	Password use	Are users required to follow good security practices in the selection and use of passwords?	
9.	Unattended user equipment	Are users required that un-attended equipment has appropriate protection?	
10.	Network access control	Protection of networked services	
11.	Policy on use of network services	Do network users only have direct access to the services that they have specifically been authorized to use? (check authorizations)	
12.	Enforced path	Are the paths from the user terminals to the server controlled?	
13.	Use authentication for external connection	Where access is available via external connections for remote users, is the access authorized?	
14.	Node authentication	Are connections to remote computer systems authorized?	
15.	Remote diagnostic port protection	Is access to diagnostic ports securely controlled?	
16.	Segregation in networks	Are controls in place to segregate groups of information services, users and information systems?	
17.	Network connection control	Is the connection capability of users restricted in networks in accordance with the access control policy?	
18.	Network routing control	Do shared networks have routing controls to ensure that computer connections and information flows do not breach the access control policy?	
19.	Security of network services	Is there a clear description of the security measures in place relating to the network services?	
20.	Operation system access control	To prevent unauthorized computer access	
21.	Automatic terminal identification	Is automatic terminal identification used to authenticate connections to specific location and to portable equipment?	
22.	Terminal log-on procedures	Is access to information services via a secure logon process?	
23.	User identification and authentication	Do all users have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual?	

No	Item	KD Reference	
24	Password management system	Is a password management system in place that provides an effective, interactive facility that ensures quality passwords?	
25.	Use of system utilities	Is the use of system utility programmes restricted and tightly controlled?	
26.	Duress alarm to safeguard users	Are duress alarms provided for users who might be the target of coercion?	
27.	Duress alarm to safeguard users	Are duress alarms provided for users who might be the target of coercion?	
28	Terminal time-out	Are in-active terminals in high-risk locations, or those serving high-risk systems, shut down after a defined period of activity to prevent access by un-authorized persons?	
29.	Limitation of connection time	Are restrictions on connection times used to provide additional security for high-risk applications?	
30.	Application access control	To prevent unauthorized access to information held in information systems	
31.	Information access restriction	Is access to information and application system functions restricted in accordance with the access control policy?	
32.	Sensitive system isolation	Do sensitive systems have a dedicated (isolated) computing environment?	
33.	Monitoring system access and use	To detect unauthorized activities	
34.	Event logging	Are audit logs produced to record exceptions and other security-relevant events and kept for an agreed period for future investigations and access control monitoring?	
35.	Monitoring system use	Have procedures been established for monitoring the use of information processing facilities and are the results of the monitoring reviewed regularly?	
36.	Clock synchronization	Are computer clocks synchronized for accurate recording?	
37.	Mobile computing & teleworking	To ensure information security when using mobile computing and teleworking facilities	
38.	Mobile computing	Is a formal policy and appropriate controls in place to protect against the risks of working with mobile computing facilities, in particular in un-protected environments?	

No	Item	KD Reference
39.	Teleworking	Are policies and procedures developed to authorize and control teleworking activities?
<b>VIII. SYSTEM DEVELOPMENT AND MAINTENANCE</b> Security requirements of systems: <i>To ensure that security is built into information systems</i>		
1.	Security requirements analysis and specification	Where new systems or enhancements to existing systems are required, are the control requirements specified?
2.	Security application systems	To prevent loss, modification or misuse of user data in application systems
3.	Input data validation	Is data input to application systems validated to ensure that it is correct and appropriate?
4.	Control of internal processing	Are validation checks incorporated into systems to detect corruption of the data processed? (are frequencies stated)
5.	Message authentication	Is message authentication used for applications where there is a security requirement to protect the integrity of the message content?
6.	Output data validation	Is data output from an application system validated to ensure that the processing of stored information is correct and appropriate to the circumstances?
7.	Cryptographic controls To protect the confidentiality, authenticity or integrity of information	
i.	Policy on the use of Cryptographic controls	Has a policy on the use of cryptographic controls for the protection of information been developed and followed?
ii.	Encryption	Is encryption applied to protect the confidentiality of sensitive or critical information?
iii.	Digital signatures	Are digital signatures applied to protect the authenticity and integrity of electronic information?
iv.	Non-repudiation services	Are non-repudiation services used to resolve disputes about occurrence or non-occurrence of an event or action?
v.	Key management	Is a key management system used, based on an agreed set of standards, procedures and methods, to support the use of cryptographic techniques?

No	Item		KD Reference
8.	Security of system files To ensure that IT projects and support activities are conducted in a secure manner		
9.	Control of operational software	During IT projects, are controls applied to the implementation of software on operational systems?	
10.	Protection of system test data	Is test data protected and controlled?	
11.	Access control to program source library	Is strict control maintained over access to programme source libraries?	
12.	Security in development and support processes	To maintain the security of application system software and information	
13.	Change controls procedures	Is the implementation of changes strictly controlled by the use of formal change control procedures to minimize the corruption of information systems?	
14.	Technical review of operating system changes	Are application systems reviewed and tested when changes occur?	
15.	Restrictions of changes to software packages	Are modifications to software packages discouraged and essential changes strictly controlled?	
16.	Covert channels and Trojan code	Is the purchase, use and modification of software controlled and checked to protect against possible covert codes and viruses etc.	
17.	Outsourced software development	Are controls in place to secure outsourced software development?	
<b>IX. BUSINESS CONTINUITY MANAGEMENT</b> <i>Aspects business continuity management: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters</i>			
1.	Business continuity management process	Is a managed process in place for developing and maintaining business continuity throughout the organization?	
2.	Business continuity and impact analysis	Is a strategy plan, based on appropriate risk assessment in place for the overall approach to business continuity?	
3.	Writing and implementing continuity plans	Have plans been developed to maintain or restore business operations in a timely manner following interruption to, or failure of, critical business processes?	
4.	Business continuity planning framework	Has a single framework of business continuity plans been maintained to ensure the plans are consistent, and to identify priorities for testing and maintenance?	

No	Item	KD Reference	
5.	Testing maintaining and reassessing business continuity plans	Are business continuity plans tested and reviewed regularly to ensure they are up to date.	
<p><b>X. COMPLIANCE</b></p> <p><i>Compliance with legal requirements: To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements</i></p>			
1.	Identification of applicable legislation	Are all relevant statutory, regulatory and contractual requirements explicitly defined and documented for each information system?	
2.	Intellectual property rights (IPR)	Have appropriate procedures been implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights, and of the use of proprietary software products?	
3.	Safeguarding of organizational records	Are important records protected from loss, destruction and falsification?	
4.	Data protection and privacy of personal information	Are controls in place to protect personal information in accordance with relevant legislation?	
5.	Prevention of misuse of information processing facilities	Does management authorize the use of information processing facilities and are controls applied to prevent the misuse of such facilities?	
6.	Regulation of cryptographic controls	Are controls in place to ensure compliance with national agreements, laws, regulations or other instruments to control the access to or use of cryptographic controls?	
7.	Collection of evidence	Where action against a person or the organization involves the law, the evidence presented shall conform to the rules for evidence laid down in the relevant law, or in the rules of the specific court in which the case will be heard. This shall include compliance with any published standard or code of practice for the production of admissible evidence. Check that the organization understands this requirement and has documented controls for such an event.	

No	Item		KD Reference
8.	Review of security policy and technical compliance	To ensure compliance of systems with organizational security policies and standards	
9.	Compliance with security policy	Do managers ensure that all security procedures within their areas of responsibility are carried out correctly and are all areas subject to regular review to ensure compliance with security policies and standards?	
10.	Technical compliance checking	Are regular checks performed for technical compliance with security implementation standards?	
11.	System audit considerations	To maximize the effectiveness, and to minimize interference to/from the system audit process	
12.	System audit controls	Are audits of operational systems planned and agreed so that the risk of disruption to business processes is minimized?	
13.	Protection of system audit tools	Is access to system audit tools protected to prevent possible misuse or compromise?	

## **10. Application of CAATs**

CAATs can be used for carrying out various types of tests involving auditee data and systems as detailed above. These can be used both for substantive and compliance testing in financial audits, performance audits as well as forensic audits.

### **Financial Audits**

**10.1** CAATs can be used in financial audits to gain assurance about the accuracy of accounts by examining the constituent transactions and records. Unlike in manual audit, use of CAATs will enable the auditor to run through the entire transactions and records and pick out samples based on statistical / judgemental methods for further detailed examination manually. Here the auditor can pick the transactions in any of the following methods:

- In a random manner (random sampling), where every record / transaction has an equal chance of getting selected; or
- Select every nth transaction (interval sampling), basically from a random start position; or
- Stratify the entire transactions / population into different strata or bands, based on the value of the item and select a specific number of transactions from each strata for further detailed checking (stratified random sampling); or
- Select high value items (monetary unit sampling)

**10.2** Some of the important tests that an auditor can carry out in financial audit using CAATs are detailed below:

• Compare transactions from month to month
• Check arithmetic accuracy of balances
• Trace the transactions from Day Books to General Ledger, Trial Balance and Balance Sheet and backwards
• Carry out an age-wise analysis of data
• Extract records fulfilling certain criteria, or above a certain monetary value for further examination.
• Identify duplicate transactions / records / invoices, etc.
• Identify and analyses gaps in transactions / records / invoices, etc.
• Reconcile amounts remitted into bank with bank statements
• Reconcile cheques paid with cheques issued
• Reconcile inter-branch transfers/remittances
• Trace the transactions from one file to another and identify cases of inconsistencies and incorrect entries
• Provide audit trail of all cash deposits, withdrawals and adjustments
• Provide audit trail of all cash disbursements
• Report cash by bank, branch, account
• Recalculate accrued income / interest receipts
• Recalculate billed amounts and identify cases of wrong billing /

under billing / over billing
• Recalculate amounts shown under sundry debtors
• Ascertain whether invoices have been raised on all relevant clients
• Summarize payments under overtime, special pay, bonus etc and look for unusual items or excess payments
• Calculate financial ratios for sales/assets, debt/equity etc.

### **Performance Audits**

**10.3** Performance audit presents ample scope for the use of CAATs. We can carry out a number and variety of tests using CAATs. For instance, with regard to Material Management and Inventory System, some of the tests that can be carried out using CAATs are as following:

• Check the time taken for processing purchase orders
• See if the electronic purchase order form is filled and complete in all respects
• Check if orders are placed on a timely basis
• See the cycle time for purchases
• Profile purchase orders by type of purchase (e.g. emergency, urgent, normal etc.)
• Profile purchases by payment type (e.g. cash, credit, advance, letter of credit, foreign currency etc.)
• Ascertain time lag between purchase requisition and placing purchase order
• Check the approvals for purchase orders with reference to the approval thresholds
• Check availability of budget for purchase of the items
• Check if the supplier database is current
• Check cases where supplier codes are different but addresses are the same
• Check cases where addresses are different but supplier codes are same
• Verify if multiple orders are placed for single items
• Check cases where purchase order date is before quotation date
• Check cases where quotation of successful bidder is after the last date for receipt of quotations
• Reconcile purchase orders with receipt of items
• Verify if the amount paid is in accordance with the approved purchase orders
• Examine the mode of payment; check all cases of cash payment
• See if advances paid are adjusted in the final price
• Identify items that are not paid for
• Check if there are any duplicate purchase orders or payments

• Analyse open orders and open invoices
• Compare the cost of items as shown in the purchase order with the cost of the item as shown in stores
• See if the quantity ordered and the quantity received is the same
• Do an age-wise analysis of inventory items
• Check the classification of items into ABC categories
• Identify if 'A' category items are classified under other categories and vice versa.
• Examine the stock levels with reference to accepted industry norms
• Review minimum / maximum stock levels and reordering levels and identify cases which are above the maximum and below minimum stock levels
• Look for case where reordering level is lower than minimum stock level
• Identify fast moving, slow moving, non-moving and dead stocks items as per approved procedures and recalculate the value of stock
• Analyse the nature of goods returned
• Check if all the stocks received are taken into account promptly
• Check if there are cases where purchase orders were issued and goods were not received
• Compare year end balances of stock with opening balances of stock for the next year
• Check cases where location of stores is not available
• Check cases of issue of stores where user codes are invalid
• Profile the issue of stores by department and by item
• Check the time taken for issue of stores from requisition date
• Check cases of double issue against single requisition
• Profile items disposed off as obsolete items from purchase date – disposed within a year, within two years, within three years and above three years
• Identify items which were scrapped and reordered immediately

10.4 The above checklist is illustrative – not exhaustive. As the auditor runs through the data and generates various hypotheses, depending on the specific procedures of the auditee organisation, numerous such analyses can be done.

### **Forensic Audits**

**10.5** These days with more and more organizations computerizing their business critical operations, CAATs are being widely used by auditors for investigating cases of fraud. Some of the tests that can be conducted by auditors using CAATs in forensic audits are as follows:

• Trace suspicious transactions across different files/databases
• Identify users who have access to the system, identify unauthorized

users in the system and the transactions initiated by them
• Unauthorized withdrawal / transfer of funds
• Unauthorized changes made to the tables/files/data by the staff in the IT/Finance/Operations Departments, System and Database Administrators etc.
• Unexplained gaps in transactions / records / bills / invoices etc.
• Identify high value items and trace them through the system. Verify if these items/ transactions were authorised by the competent authority
• Identify items where data entry was done outside normal office working hours
• Analyse employee overtime payments
• Check health claims of employees for significant amounts
• Identify loans in excess of collateral value
• Analyse sales returns after the end of the accounting period
• Analyse sales returns after a sales contest
• Examine cases where there is sudden activity in dormant accounts
• Check for duplicate addresses relating to,
✓ Employees
✓ Vendors
✓ Customers
✓ Debtors
✓ Check duplicates relating to,
✓ cheques issued
✓ invoices/bills processed
✓ payments made
✓ accounting entries passed
• Check multiple orders to a vendor for purchase of a single item
• Check invoices with dates prior to purchase order dates
• Profile large individual payments
• Check payments to vendors who do not exist in vendor database
• Verify all disbursements in cash
• Check all negative balances accounts
• Review gaps in cheques with cheques declared void
• Reconcile cheques issued with checks accounted for
• Check unusual items like debit balances in payables, credit balances in receivables

## **Data Downloading**

**10.6** Since many of our auditees use Oracle databases, the procedure for downloading the data from such databases into IDEA and MS Access is given below. Although data downloading through ODBC is generally favoured by auditors, some auditees prefer to

provide data in other formats like ASCII, since they design and run their Oracle databases using older generation languages like COBOL. Therefore, this guide provides a step-by-step procedure for downloading data from Oracle database into IDEA and Access using both ODBC connectivity and by creating a record definition (for ASCII fixed length format).

### **10.7 Procedure for Setting up ODBC Connectivity**

- The auditor needs to have the necessary network client software installed on his/ her desktop
- The appropriate network protocol (generally TCP/IP) has to be installed on the desktop along with the network address (IP address)
- Since Windows is the standard operating system on all the desktops in IAAD, the auditor can load the ODBC driver manager and the ODBC drivers (especially Oracle driver) on the desktop by installing the latest version of Microsoft's 'Data Access Components'. ODBC Oracle drivers are also available from Oracle Corp. itself, as well as from other third party vendors.
- In order to access the Oracle database, Oracle client and the networking components are also to be installed on the auditor's PC. It may be ensured that the client and the database versions of Oracle are the same.

**Note:** ODBC connectivity does not require the connecting systems to be running the same operating system but the protocols should be the same.

**10.8** Once the ODBC connectivity is set up, data can be downloaded from the Oracle database to different generalized audit software tools as detailed below:

### **10.9 MS Access**

- Open MS Access
-  Select 'Get External Data' from 'File' menu
-  Select 'Import / Link Tables'
-  Select 'ODBC Databases' in the file format
-  Choose 'Machine Data Source'
-  Select the data source if it is available on the screen or else select 'New'
-  Select 'User Data Source'



- Select 'Microsoft ODBC for Oracle'



- Specify the 'User Name', 'Password' and 'Server Name' in 'Microsoft ODBC for Oracle Connect'



- Having entered the user name, password and server name in the 'Microsoft ODBC for Oracle Connect', the auditor can view all the available tables in the auditee server and can then choose the required tables to be imported.



- Specify an appropriate name for the database to work on the tables thus imported.

**Note:** **Importing** implies that the file/table is physically transferred onto the auditor's file structure whereas, **linking** establishes only a logical connection between the file / table and the auditor's file structure. It is advisable to import the files / tables rather than establish a link to the file /table in the auditee's database, since any changes made inadvertently by the auditor to the data will impact the auditee's database.

**Generally, data from an Oracle database is imported / downloaded through an Open Database Connectivity (ODBC) since it is a standard method of sharing data between databases and programmes and the ODBC drivers use the standard SQL to access external data.**

In order to access data from any ODBC data source, the auditor needs to be set up as a user in the concerned system by the Database Administrator (DBA) of that system (in this case, the VLC system) with appropriate permissions. Also, an ODBC Data Source Name (DSN) must be defined on the VLC system to enable the auditor to access the system.

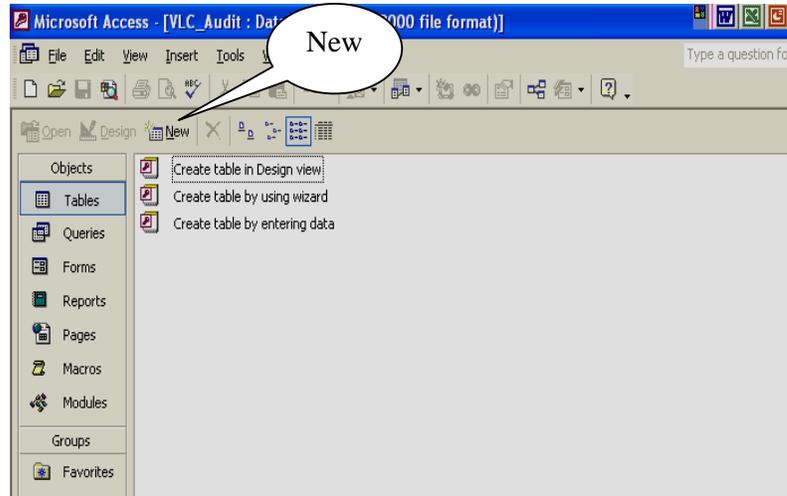
There are three kinds of ODBC Data Source Names as detailed below:

- **User** – this type of DSN stores its information in the system registry on a user-by-user basis. User DSNs are available only when the corresponding user is logged on to the computer.
- **System** – this DSN also stores its information in the system registry but it is available irrespective of whether anybody is logged on or not.
- **File** – this DSN is also available irrespective of who is logged on. It is not stored in the system registry but in an ordinary text file.

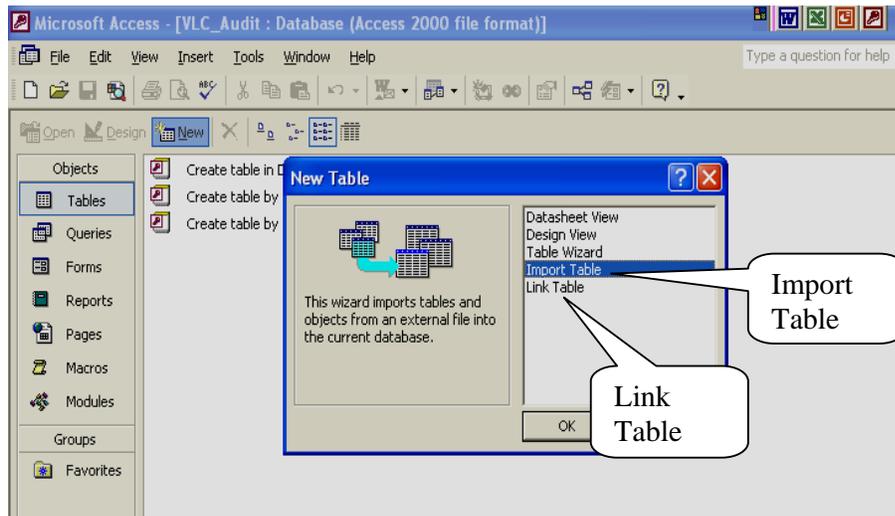
**10.10** The ODBC data source once created, can be used to import the Oracle data tables from that Server any number of times until the access is blocked by the DBA. Once the ODBC connectivity is set up, data can be downloaded from the Oracle database to Microsoft Access as detailed below:

**10.11 Importing Data in to MS Access**

- Create a new Database named ‘**VLC Audit**’ in MS Access
- In the Tables Module, click **New** as shown below.



- You will get a **New Table** dialog box as shown below.



- Select **Import Table** (If you intend to have only a link to the tables, you can choose **Link Table**)

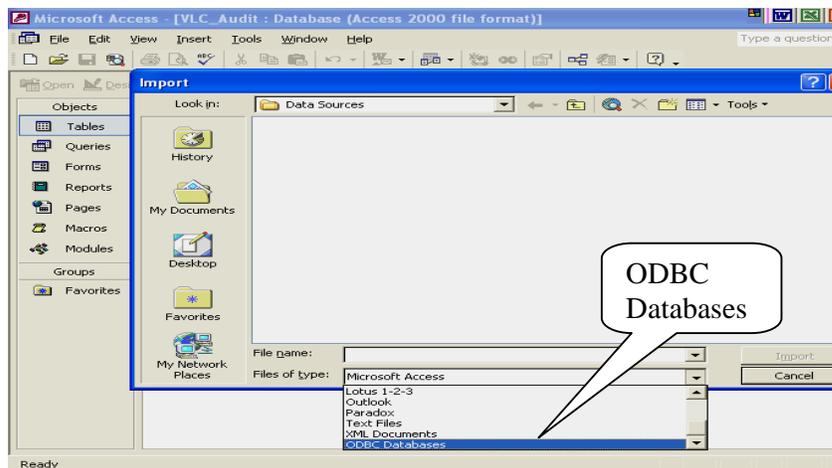
**Note: Importing** implies that the file/table is physically transferred onto the auditor's file structure whereas, **linking** establishes only a logical connection between the file / table and the auditor's file structure.

It is advisable to import the files / tables rather than establish a link to the file /table in the auditee's database, since any changes made inadvertently by the auditor to the data will impact the auditee's database if the table is linked.

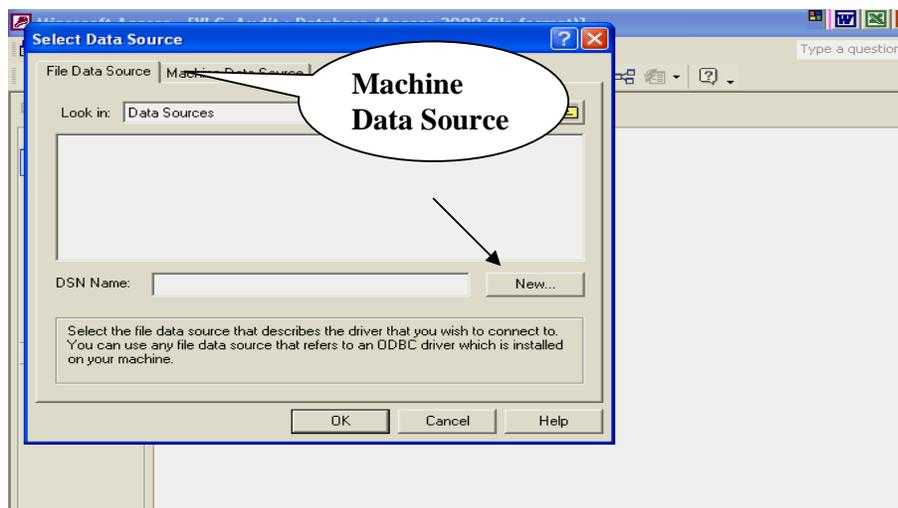
Also, improperly designed queries on linked tables could adversely impact performance.

➤ Click **OK**

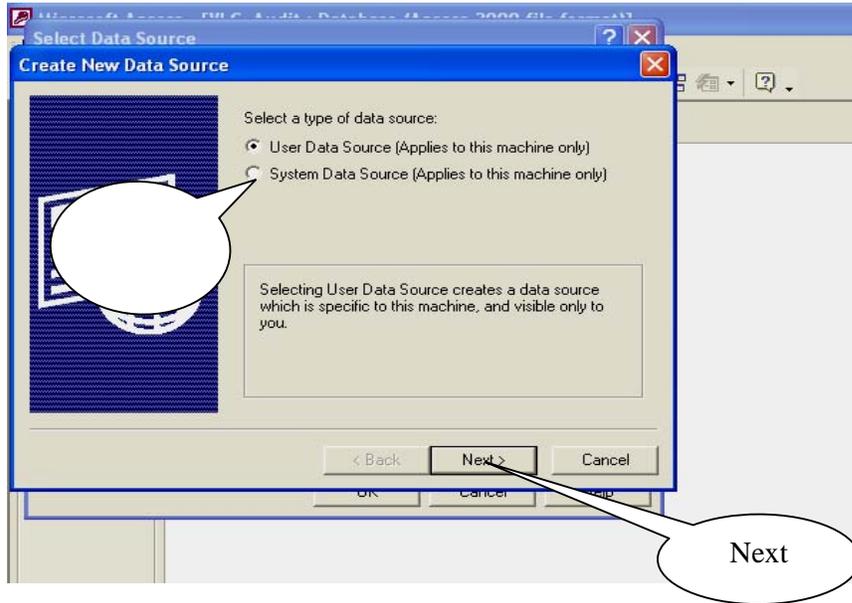
You will get an Import dialog box. Select '**ODBC Databases**' in the file format as shown below.



You will get a Select Data Source dialog box. Here select **Machine Data Source**. If the Data Source has been created earlier and is available, you can choose it; or else, create a new Data Source by clicking **New**.

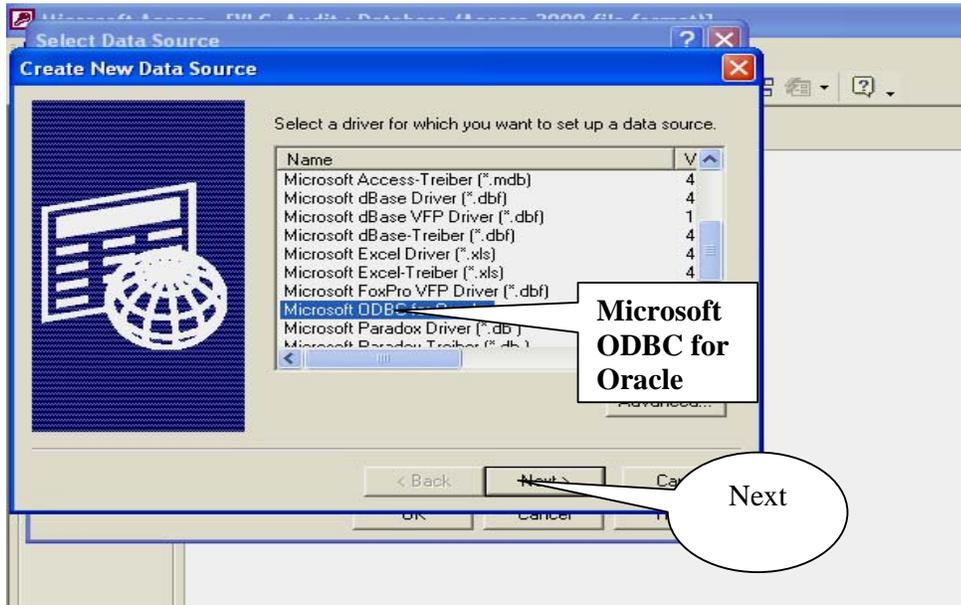


You will get a **Create New Data Source** dialog box. Select **User Data Source** and press **Next**.

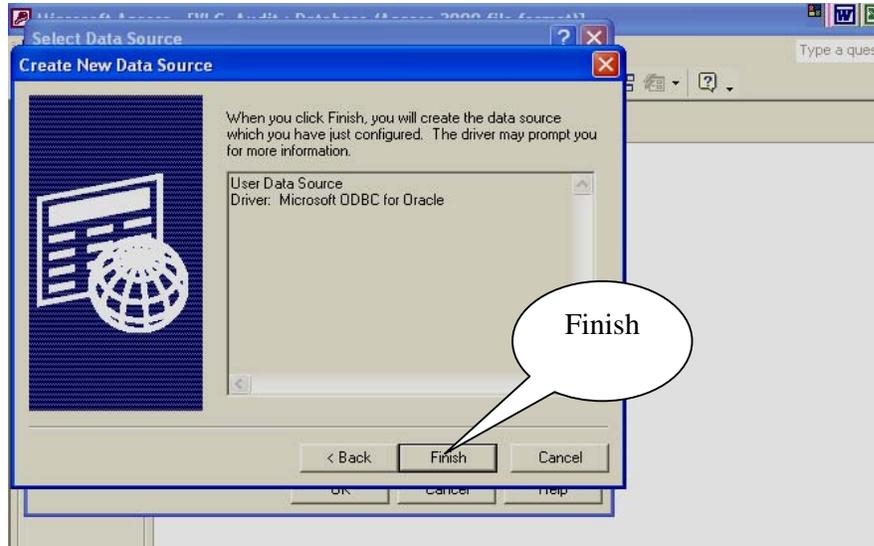


**Note:** User data source creates a data source that is specific to the machine you are using, and is visible only to you. On the other hand, system data source creates a data source specific to the machine you are using but usable by any user who logs on to this machine.

You will then see the following screen, wherein you have to select the driver for which to set up the data source. Select **Microsoft ODBC for Oracle** and press **Next**.



You will then see the following screen, where you need to click **Finish** to create the data source.



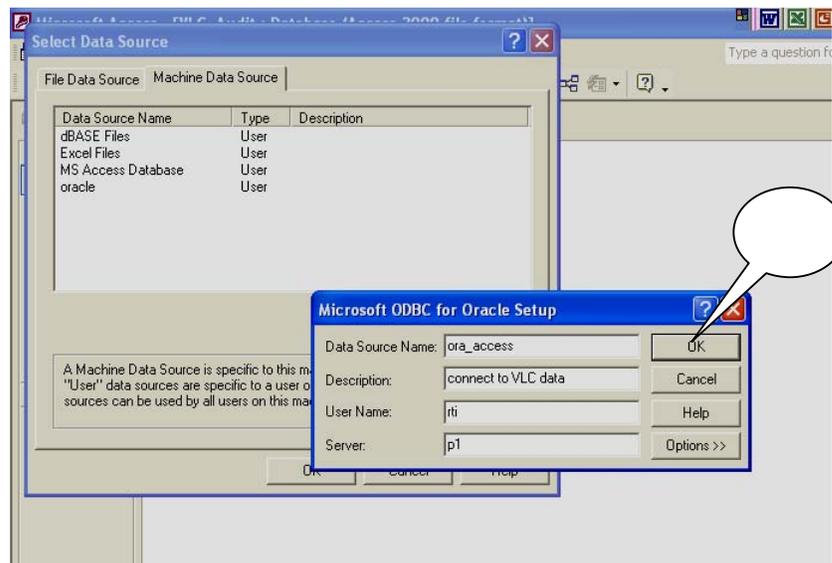
You will see a **Microsoft ODBC for Oracle Setup** dialog box as shown below. Type the following:

**Data Source Name:** Specify a name (this is user defined) .Let us say, **acc\_oracle** in this case.

**Description:** Give a description to the connection you are setting up (this is user defined).  
Let us say, **connection to VLC database** in this case.

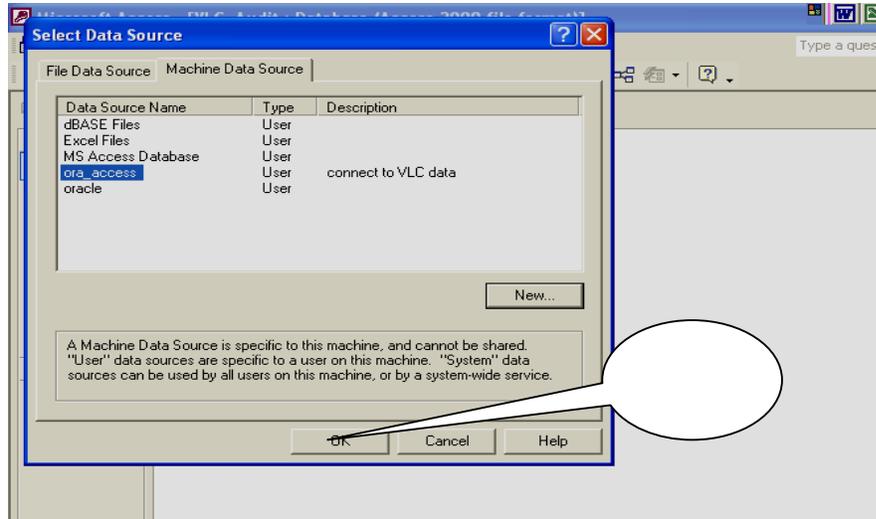
**User Name:** This is mandatory and has to be obtained from the DBA

**Server:** This is also mandatory and has to be obtained from the DBA



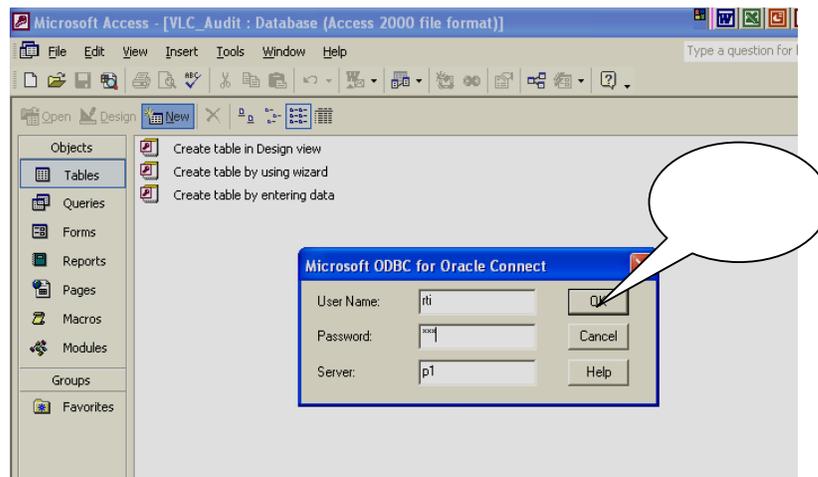
Press **OK**.

You will see the new **Machine Data Source** as shown below. Select it (**ora\_access** in this case) and press **OK**

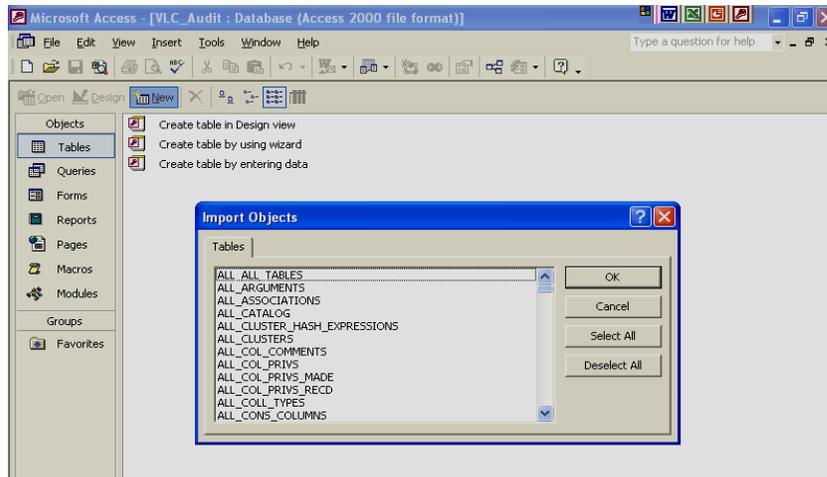


You will see a **Microsoft ODBC for Oracle Connect** dialog box.

- Type the **user name, password and the name of the server** (these are to be obtained from the DBA).
- Press **OK**.

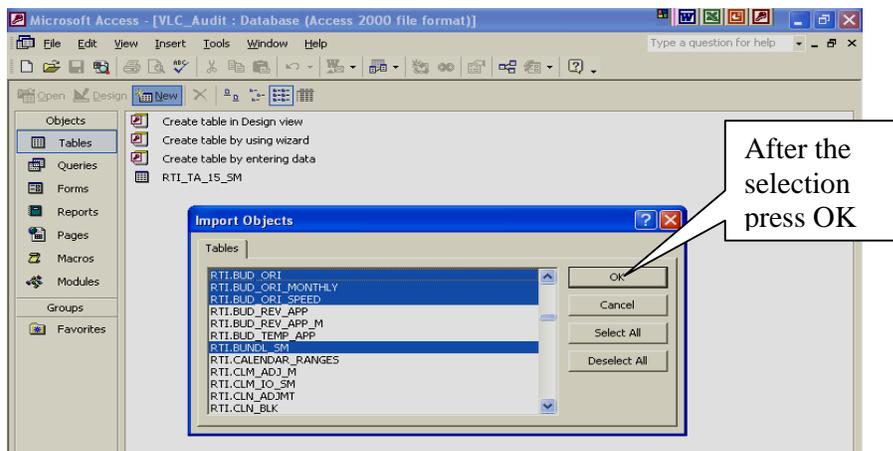


The **Import Objects** dialog box comes on. You can view all the available tables in the VLC server and can then choose the required tables to be imported.

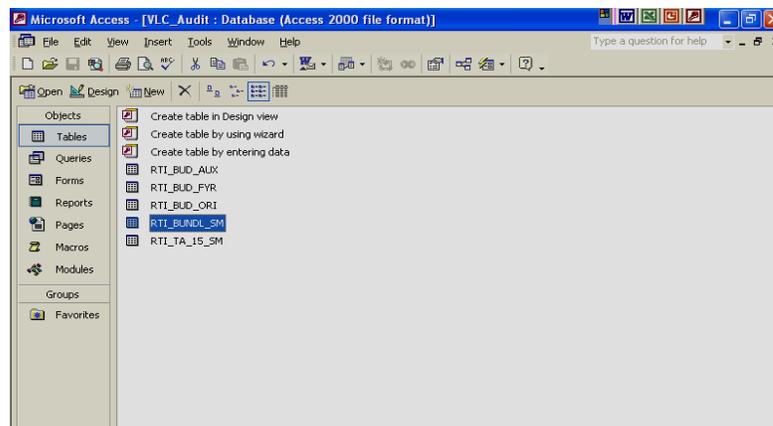


You can select more than one table at a time by holding down the Shift key and pressing the down arrow.

- Press **OK** after completing the selection of tables.



The tables will be imported into your Access database as shown below.



## 10.12 Verification Procedures

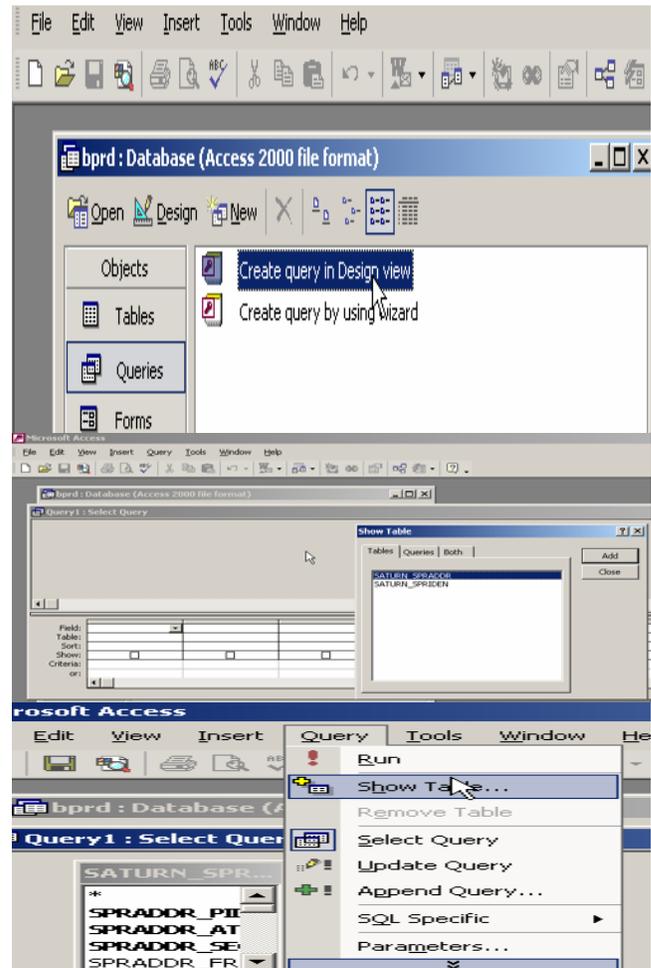
After downloading the required data, the auditor has to verify it to ensure that what has been downloaded is the correct data and that it is **complete** (not dummy or incomplete data), **valid** (not junk or irrelevant data) and **accurate** (represents the actual transactions). This is done by reconciling the data with the details provided by the auditee as detailed below:

- Obtain the actual **number of records** contained in the auditee database and compare it with the number of records downloaded; in respect of RDBMS, this should be done for all the tables;
- Obtain the control totals or hash totals from the auditee and compare with those of the downloaded data;
- Cross check totals and balances with reference to actual documents/print outs from the auditee.

### MS ACCESS and MS EXCEL as Audit Tools

Click on “Queries”  
and then  
“Create query in Design view”.

Select the tables you want for your query  
and click add.  
(If you need to add more tables later click on  
the Query menu > Show Tables.  
Select the tables you want for your query  
and click add.  
(If you need to add more tables later click on  
the Query menu > Show Tables.

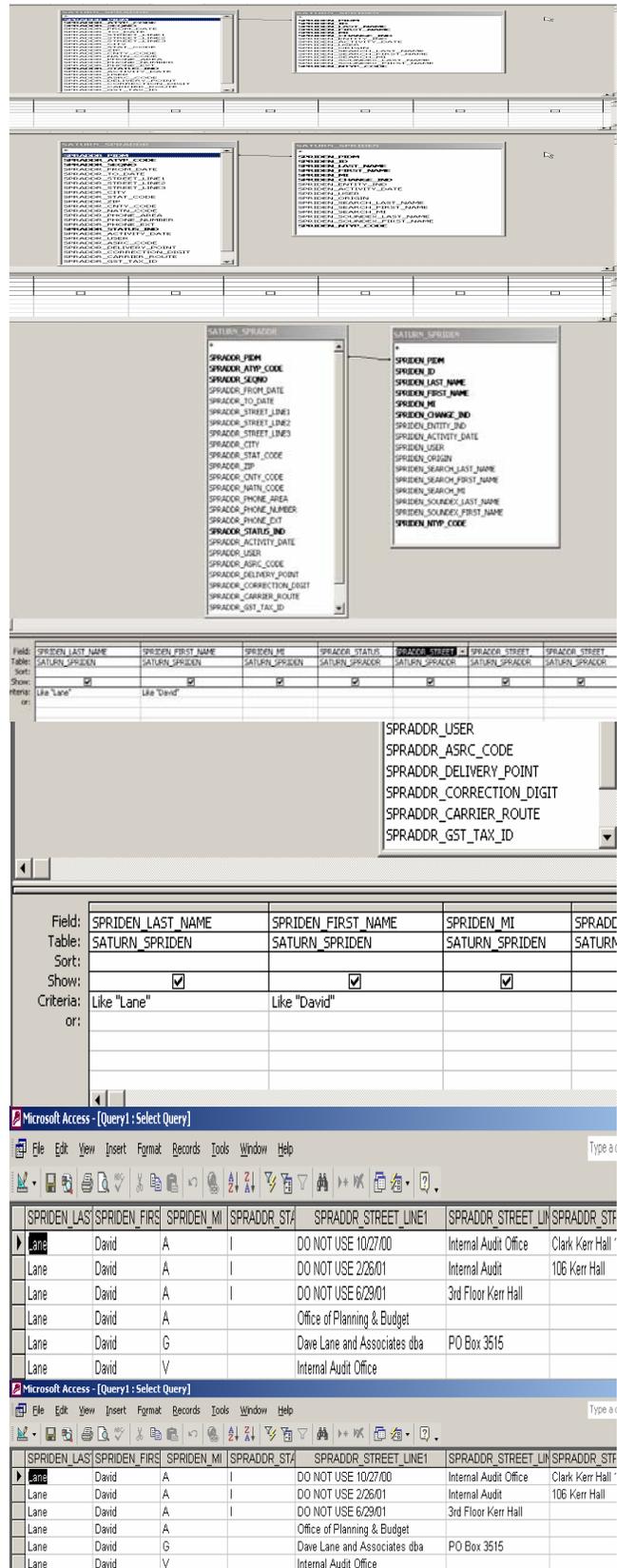


The table you added appear at the top of the design query screen. These table must be joined by dragging and dropping from a data field in one table to a data field in the other table. This is an inner (equality) join were the field values in both tables are the same.

Data fields are added to the query by double clicking or dragging and dropping them to the lower window on this screen. If you want to find out what type of data is in a table you can select all the fields on that one table (with no joins to other tables) and run the query. This will help you determine appropriate fields to join.

Criteria can be defined for any field. Criteria include greater than (>), less than (<), “like”, “and”, and “or” to name a a few common operators. See MS Access Help for more information. The “Like” operator allows for non-exact matches (unexpected use of capital letters, etc.) Adding the criteria “Is Null” to a given column eliminates all records which have no value in that column

The query returns the results, below. These results can be copied to an Excel Worksheet by highlighting the header row and selecting Copy

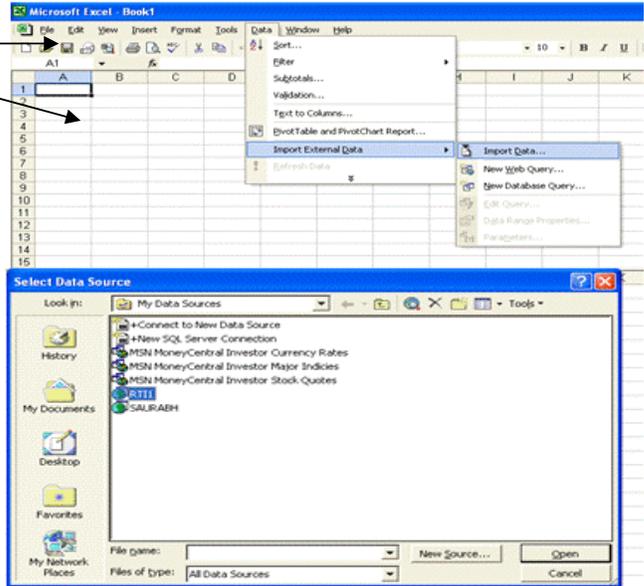


**Excel as Audit Tool**

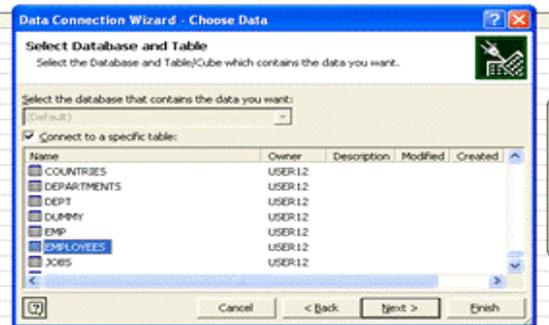
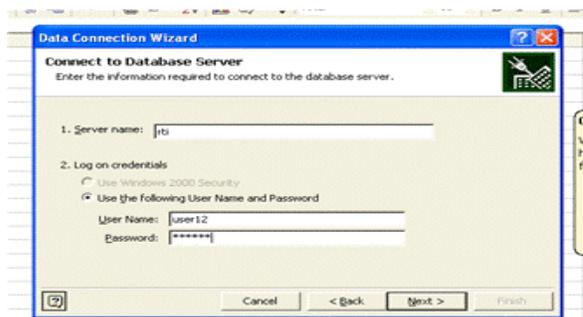
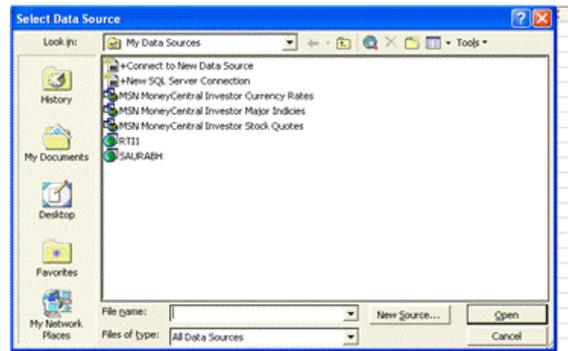
**Importing Oracle Data into Excel**

Select Import External Data > Import data

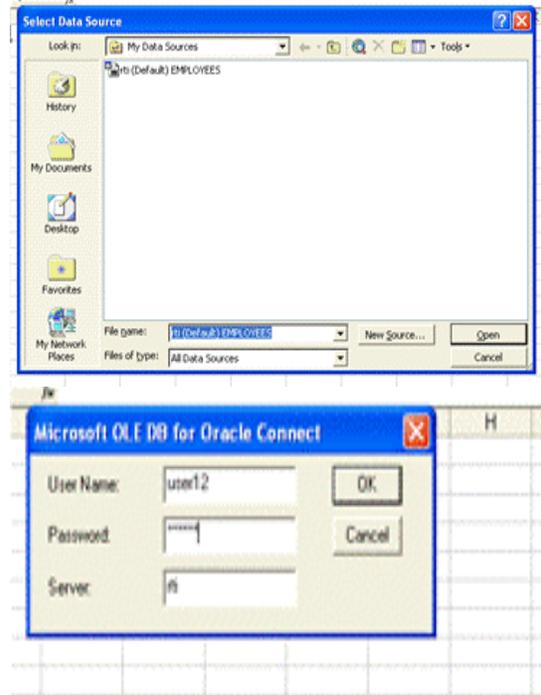
Select the data source. Existing or new Data Source will have to be used. Connect to the database using the Oracle database userid and password in case of existing data source.



In case a new Data source is to be created, click on the “New Source”. The Data Connection Wizard appears. Supply server name, user name and password of the database you are trying to connect to.

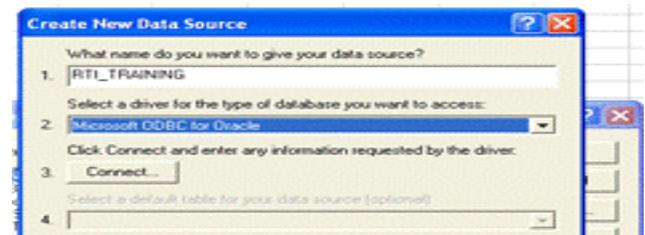
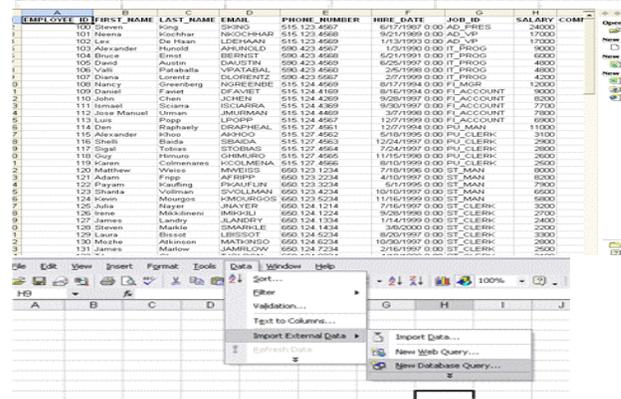
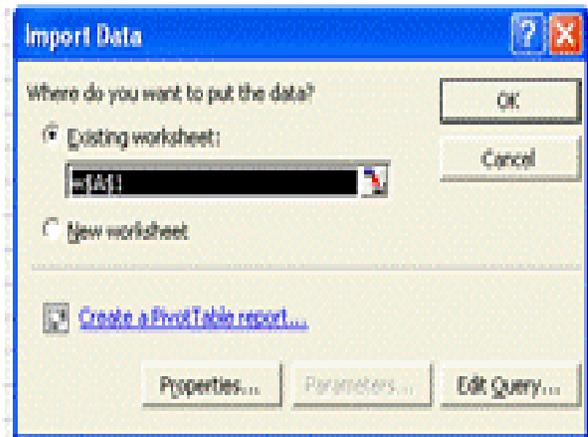
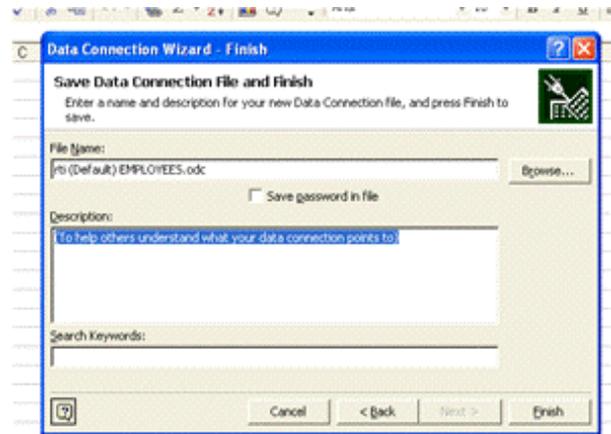


Having selected the required table, save the data connection file. The Data Connection File is now available as a data source allowing the User to connect to the Oracle database thru' MS EXCEL. This source can now be selected.



The system again confirms the user name and password. Thereafter, the table data is imported into the worksheet. This data can be then analyzed.

Database queries can also be run in Excel without importing data from Oracle. This requires installation of MS Query. Select Import External data>New Database query. Select the Access database. The MS Excel now connects to the database

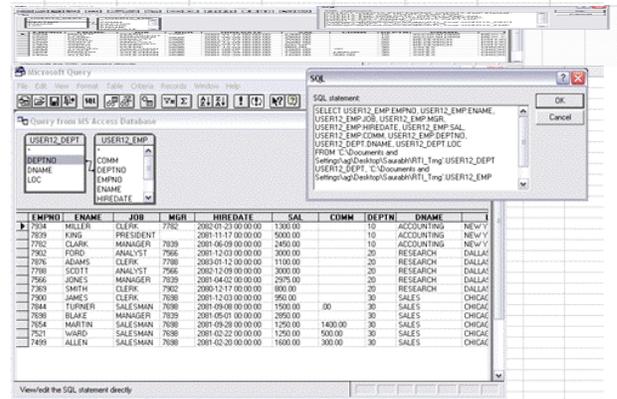
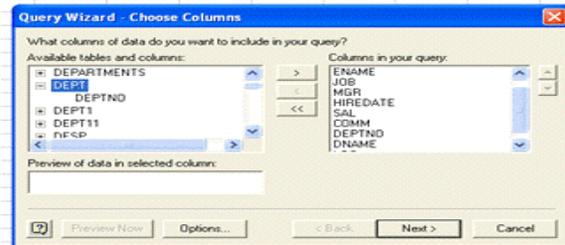
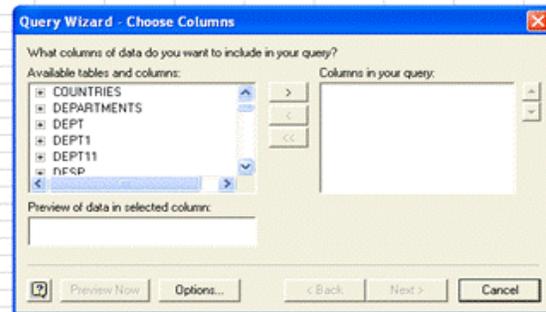
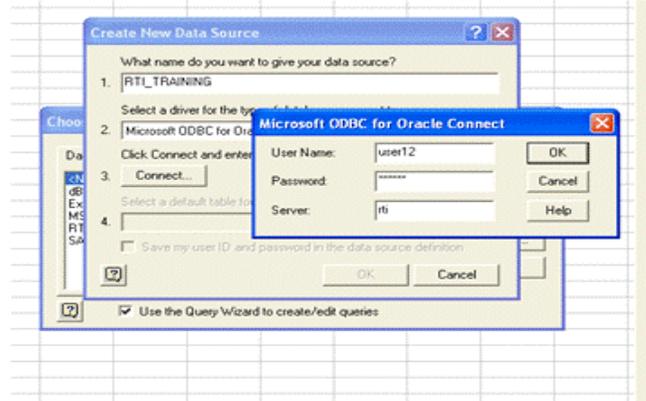


8. Provide the database particulars such as username, password and the server in which the database resides. This process is similar to the one adopted for creating a new DSN for Oracle databases in MS Access

Provide the database particulars such as username, password and the server in which the database resides. This process is similar to the one adopted for creating a new DSN for Oracle databases in MS Access

The Query wizard now displays the tables available in Oracle database that could be queried. Select the columns required. If more than one table are required, the relationship between them has to be established using MS Query

The MS Query is similar to MS Access query tool. It allows creating queries joining multiple tables; setting criteria and exporting results to MS Excel. The query output can also be used in generating pivot reports and charts



## **Procedure for Downloading Data in ASCII Format**

### **Importing ASCII Fixed Length File into IDEA 2002**

**10.13** The mode of importing an **ASCII fixed length** file is detailed below:

- Open IDEA.



- Select '**Import Assistant**'



- **Select the data file** to import from or **click ...** to browse for the file name. The file can be located anywhere - hard disk, CD ROM, Tape, USB drive, etc.



- Next **select the import method**. Various formats like ASCII (fixed length and delimited), EBCDIC (fixed length), SAP/AIS, Print report files, ODBC sources, Access, Excel, dBase, AS 400, etc. can be imported into IDEA. While any of these methods can be selected, let us select ASCII fixed length format.

**10.14** For ASCII (fixed as well as delimited) and EBCDIC (fixed length) data has to be defined to IDEA in terms of size, type and number of fields. This is called '**Record Definition**'.

*Note:* If you have previously created and saved a record definition for the data file either through the Import Assistant or through RDE (the Record Definition Editor), you can use the option '**Use/change an existing record definition**'. This option can also be used to change an existing record definition, if incorrect. Note that if you wish to add calculated (virtual) fields to the definition, you must use the RDE option to amend the definition.

- '**Import Assistant**' will try to determine the type of the data file as given below. Accept if what the import assistant says is acceptable; or else change the name of the data file format to the correct format.



- Click the '**Fixed Length ASCII**' button and then press '**Next**'. You will get a screen asking for **Record length**. Again press **Next** button. You can accept what the import assistant gives or correct it.



- Press '**Next**' and follow the directions on the screen.



- This leads us to the next screen where you can change the width of the data field by dragging with mouse



- Once you are happy with the selection, click '**Next**'.



- You will have the option of '**Linking**' the file or '**Importing**' the file. Choose '**Import**', since IDEA runs faster when the file is imported in to its structure.



- Give a specific name to the '**Record Definition**' and the '**Database**'.



- Click '**Finish**'.

### **Importing ASCII Fixed Length File into Access**

**10.15** The procedure for importing a text file into Microsoft Access is as following:

- Open Access



- Go to '**File**' and select '**Get External Data**'



- Select '**Import**'



- In 'Files of type' choose '**Text Files**' and **select the file** that you want to import in to Access



- You will have the option to select 'Delimited' or 'Fixed Width' data. Import Text Wizard suggests the type of data based on its reading of the file. You can either accept it or change it to the other type as given therein.



- Press '**Next**'



- Specify the field breaks by clicking and dragging the line to the place /field width that you want or accept what the Import Text Wizard suggests



- Click 'Next'



- Choose the first option suggested by Import Text Wizard i.e. ‘store the data in a new table’ as there is a possibility of having errors in rows and records in case you choose to store the data in an existing table and click ‘Next’



- You will see the following screen, where you can make changes to the ‘Field Name’ and the ‘Data Type’ (text, numbers, currency, memo, data etc.). You can also decide whether you want to import all the fields or leave out some of these.



- You are given an option for defining a ‘primary key’ (unique information which does not contain/accept duplicates) in the table. You can specify any particular field as primary key or let Import Text Wizard choose it for you. You also have an option of not having a primary key.



- Click ‘Next’. In case you want the Import Text Wizard to analyse the table for you (to check on duplicates and data consistencies), you can click on the relevant check box on your screen and click ‘Finish’. If not, in any case, click ‘Finish’.

### Downloading Other Data Types

**10.16** Part from the data types mentioned above, both IDEA and Access can download data from a variety of data types like Microsoft Excel, Access, dBase, Paradox, Lotus 1-2-3 spreadsheets, XML (Extensible Markup Language) and other programmes and databases that support ODBC. Both the packages offer extensive ‘Help’ Functions and the mode of downloading data from these data types is available in the respective help menu.

### Verification Procedures

**10.17** After downloading the required data, the auditor has to verify it to ensure that what has been downloaded is the correct data and that it is **complete** (not dummy or incomplete data), **valid** (not junk or irrelevant data) and **accurate** (represents the actual transactions). This is done by reconciling the data with the details provided by the auditee as detailed below:

- Obtain the actual **number of records** contained in the auditee database and compare it with the number of records downloaded; in respect of RDBMS, this should be done for all the tables;
- Obtain the control totals or hash totals from the auditee and compare with those of the downloaded data;
- Cross check totals and balances with reference to actual documents/print outs from the auditee.

## Documentation

**10.18** Both IDEA and MS Access offer facilities for documenting the work of the auditor with regard to downloading and analysis of data. This not only provides key audit evidence but also facilitates review of the quality of the auditor’s work by peers and superiors.

### IDEA

**10.19** The ‘**History**’ view in IDEA keeps a record of every operation performed by the auditor. It maintains an audit trail of all the activities carried out on the file/database and logs the details of the files imported into IDEA along with the time and date of import, extractions carried out, records extracted, and the step-by-step process of all the tests run on the data. ‘**History**’ view can be used by the auditor to recheck the queries in case the results are not as per expectations, or to verify where the query has gone wrong. Print out of these views form part of the working papers of the auditor and can help in planning future audits of the same organisation or similar area of another organisation. IDEA Script code can be copied from these views to a Macro Window to automate repetitive tests. This code can also be added to the IDEA Toolbar for ease of use.

### MS Access

**10.20** The ‘**Documenter**’ function in Access facilitates documentation of all the files in all the modules of Access like tables, queries, forms, reports etc. For instance, if you want to document a table in the database, you can get a view of all the fields in the table along with the table properties, relationships existing with other tables, data types, sizes, index details etc.

**10.21** The SQL view of the tests carried out on the data can be viewed as follows:

- Go to a specific query in Access and open it in the ‘**Design**’ view;
- In the ‘**View**’ menu, click ‘**SQL View**’.

The SQL view provides the details of the query in an easy-to-understand form. Like the ‘**History**’ view of IDEA, ‘**SQL view**’ in Access can be used to provide key audit evidence of the tests carried out by the auditor and can also be used for planning future audits and running repetitive tests relating to the same organisation or similar area in another auditee.

## Using SQL for Querying Data

<b>Table(s)</b>	Relational Databases are so designed (using the principles of normalisation) that in many, if not most, cases, the data of interest to the auditor comes from two or more tables. For the purposes of querying, the auditor has to “join” the tables on one or more common or related fields.  In SQL there are two types of joins: <ul style="list-style-type: none"><li>• “<b>INNER JOIN</b>”, which retrieves data from both</li></ul>
-----------------	---

	<p>tables where the values in the common fields are matched. Note that the data in either table, which does not have a corresponding match in the other table, is not retrieved.</p> <ul style="list-style-type: none"> <li>• “<b>OUTER JOIN</b>”, which retrieves all data from one table, in addition to the matched data from the other table.</li> </ul>
<b>Fields</b>	<p>A large variety of fields can be retrieved:</p> <ul style="list-style-type: none"> <li>• All or some of the fields from the table (or joined tables) can be retrieved</li> <li>• Calculated fields, using a variety of functions, can be retrieved. Common calculated fields include,</li> <li>• Fields using <i>summary operators</i> like average, count of records, maximum, minimum etc.</li> <li>• Fields involving <i>date manipulation</i> e.g. calculating age from the date of birth field and the system date</li> <li>• Fields involving string or <i>text manipulation</i> e.g. looking for particular names or words.</li> <li>• Fields involving <i>mathematical functions</i> e.g. rounding off of numbers.</li> </ul> <p>In addition, if the auditor possesses some programming knowledge, he/she can generally write his/her own ‘user-defined functions’ and ‘procedures’ in common programming languages like Visual Basic or C, and further refine his SELECT queries.</p>
<b>Sorting</b>	<p>The results of the SELECT statement can be sorted on any particular field, using the “<b>ORDER BY</b>” clause. The sorting can be either in ascending or descending order.</p>
<b>Conditions</b>	<p>The ‘<b>WHERE</b>’ clause in the SELECT Statement is not limited to just one condition. The auditor can specify a multiplicity of conditions, as well as the interrelationship between the conditions (e.g. the conditions are all required to be satisfied, or only one condition is necessary. These conditions can be combined using operators like “<b>AND</b>” or “<b>OR</b>”</p>
<b>Group</b>	<p>A very powerful feature of the SELECT syntax is the “<b>GROUP BY</b>” clause. For example, if we wish to know the number of employees by Grade, we would use the clause “<b>GROUP BY Grade</b>”, and then select a calculated field using a summary operator, namely count of Employee IDs.</p> <p>Linked to the “<b>GROUP BY</b>” clause is the “<b>HAVING</b>” clause.</p>

	While the “ <b>WHERE</b> ” clause applies the relevant condition to the underlying data in the tables, the “ <b>HAVING</b> ” clause applies the condition to the results of the summarisation performed using the “ <b>GROUP BY</b> ” clause. For example, in the case described above, we could use the “ <b>HAVING</b> ” clause to restrict the results only to grades which have 20 or more employees.
<b>Operators</b>	A large number of mathematical and Boolean operators can be used to refine conditions in the “ <b>WHERE</b> ” clause. These include: <ul style="list-style-type: none"><li>• <b>Equal to, Greater than, Less than, Not equal to</b></li><li>• <b>Greater than or equal to, Less than or equal to</b></li><li>• <b>Between... And...</b></li><li>• The “<b>IN</b>”, “<b>EXIST</b>” and “<b>LIKE</b>” keywords</li></ul>
<b>Sub-queries</b>	The auditor can combine the results of different SQL statements by ‘nesting’ one SQL statement within another SQL statement and so on.

The combinations of different clauses and options listed above can be used to create innumerable variations of the SELECT statement, which can be used to satisfy almost all the data analysis requirements of the auditor.

## **10.22 Oracle Utilities**

Oracle provides utilities to back up an Oracle database and also to move data between Oracle databases. It also enables to load the data into the tables from the operating system files.

### **Export**

Export writes the information from the tables and data objects into operating system files. The files Oracle creates are called **DUMP** files. This **DUMP** files are in Oracle Binary format, which can be only used by Oracle Import utility. If no filename is specified while creating an export file, then by default it is called as **EXPDAT.DMP**.

### **Import**

Import process extracts the database objects and data saved to an Oracle export file and imports them into a specified database. Oracle import utility is used to extract data from the export file **EXPDAT.DMP** and thus help in exporting the data from **Database(1)** to **Database (2)**.

Privileges required

Before using the Export utility, one has to check for storage space on the disk or tape so that the export files can be written to the disk. If the disk space is not sufficient, Export utility terminates with a write failure error. To use Export, one must have the **Create Session privilege** on an Oracle database. To export tables owned by another user, one **must have the exp\_full\_database** (full database Export) role **enabled**.

Import utility can read from those files, which were created using the export utility. If the export file is a full database export, then it will only be possible to import that file **if you have the imp\_full\_database** (full database Import) role **enabled** (this role is granted to user when an user is created)

As files created by Export are stored in a special format, no other Oracle utility other than Import can use them. Also data cannot be transferred to Non-oracle systems using these utilities.

Export/Import mode

Objects that are exported/imported depend on the type of object chosen. The objects that can be exported/imported are:

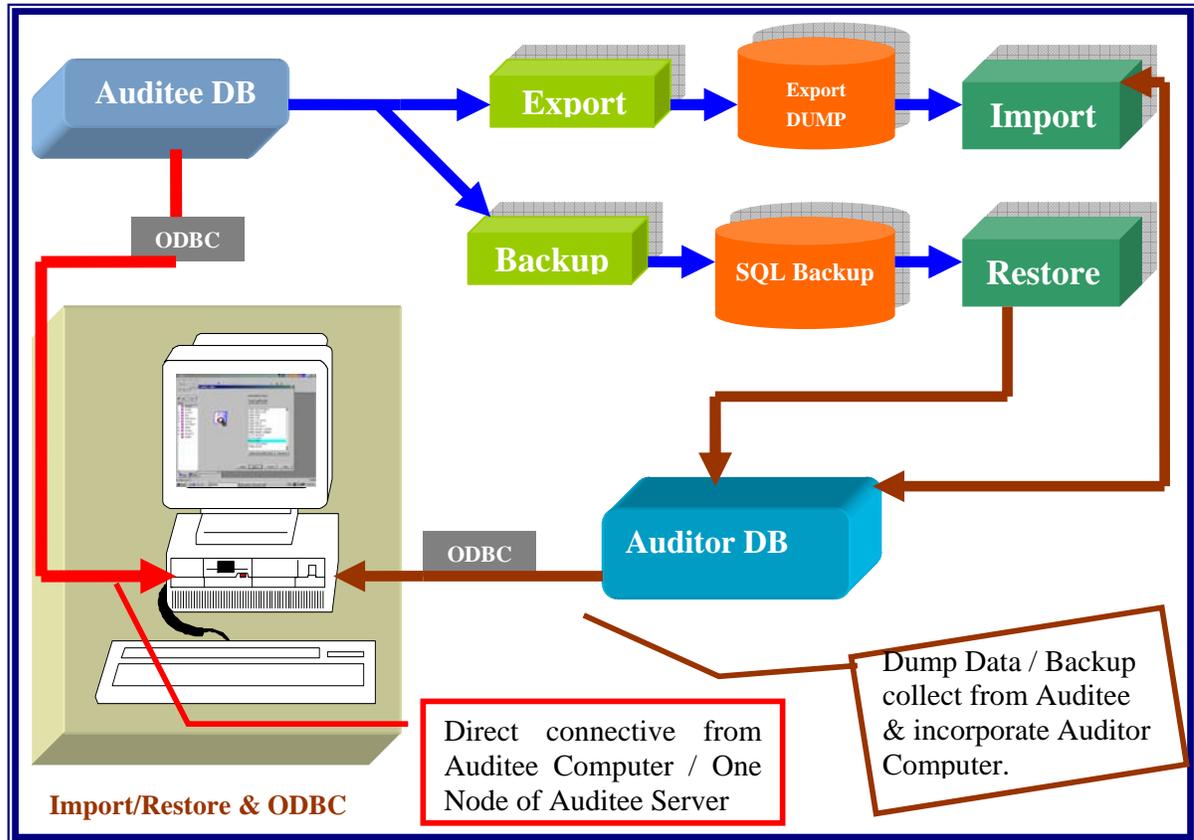
Table:           this allows export/import the specified tables rather than all tables. Default setting is export/import of all tables belonging to a particular user.

User:            this allows to export/import all objects i.e. tables, data, indexes etc. A privileged user exporting/importing in this mode can also export/import all objects belonging to other users.

Full Database: only users with the **exp\_full\_database/ imp\_full\_database** role can export/import in this mode. All database objects can be exported/imported in this mode. Only DBA can use this mode.

From **DOS/COMMAND** Prompt

**C:\> exp for export C:\> imp for import** : System prompts for a username and password. Enter username and password to begin an interactive session. The interactive export/import session prompts the user for the information it needs. Press the enter key to accept the default values or enter the new values as required.



## EXPORT

Exporting of ORACLE database objects is controlled by parameters. To get familiar with EXPORT parameters type:

**exp help=y**

You will get a short description and the default settings will be shown. The EXPORT utility may be used in three ways:

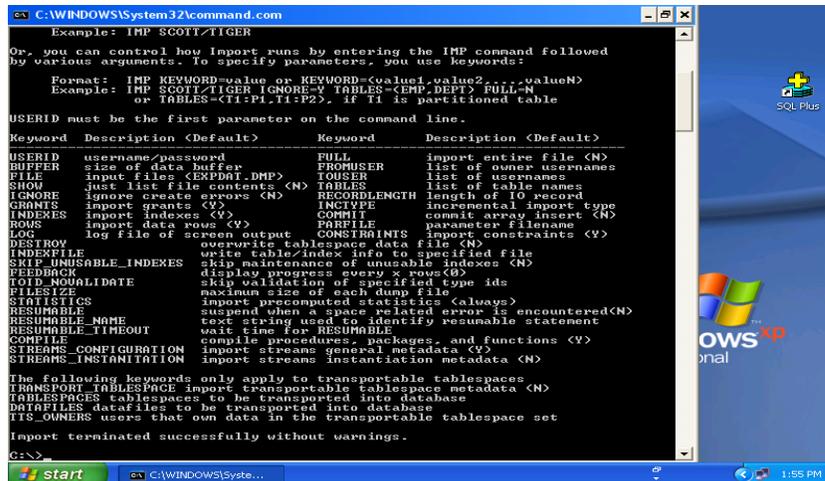
- Simply type **exp**. You will be prompted for your ORACLE userid, password. All other prompts answer by pressing the return key. This is the easiest way to export all data you stored in the ORACLE database. You may assign other values than the defaults to the parameters but in most cases it is unnecessary.
- Example of exporting scott's tables EMP and DEPT to file **TEST.DMP**:
- **exp naithani/scaithani file=TEST.DMP tables=(EMP,DEPT).**

About to export specified tables ...

```
. exporting table          EMP          14 rows exported
. exporting table          DEPT          4 rows exported
Export terminated successfully without warnings.
```

## IMPORT

IMPORT utility is controlled by parameters. To get familiar with these parameters type: **imp help=y** You will get a short description of usage and default settings of parameters.



To start IMPORT simply type **imp**. You will be prompted for your ORACLE userid, password. The next prompts depend on what you answer. In most cases you may answer the prompts by pressing the return key. But the following prompts you have to answer carefully.

**Import file: expdat.dmp >**

If your data was exported to file expdat.dmp press return, otherwise enter the filename where the exported data resides.

**Ignore create error due to object existence (yes/no): yes >**

This is a flag to indicate how object creation errors should be handled. If you import into an existing table and you set IGNORE=Y, rows could be duplicated if they were already present in the table.

**Import entire export file (yes/no): yes > no**

Username:

If your exportfile consists of more objects than you want to import, enter no. In this case you will be prompted for the Username (this is normally your ORACLE account).

**Enter table names. Null list means all tables for user**

Enter table name or . if done:

After entering the username you will be prompted for table names until you press the return key without entering a table name. Then IMPORT will be started.

Instead of the dialogue method you may use parameters. This is analogous to the methods described for EXPORT.

Examples:

**imp <naithani/scnaithani> tables=(EMP,DEPT)**

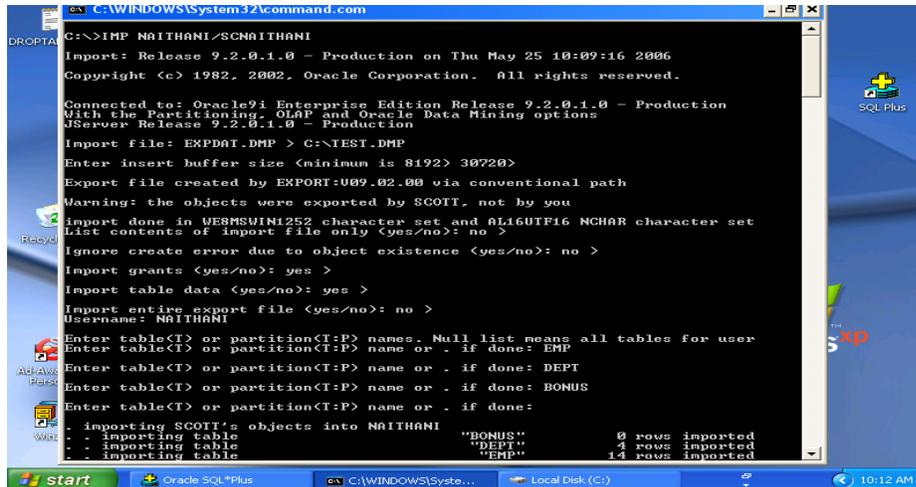
Tables **EMP,DEPT** will be imported from the default file **TEST.DMP** into the database.

After importing you should get messages like:

```

importing SCOTT's objects into SCOTT
. importing table "DEPT"                4 rows imported
. importing table "EMP"                 14 rows imported
  
```

Import terminated successfully without warnings.

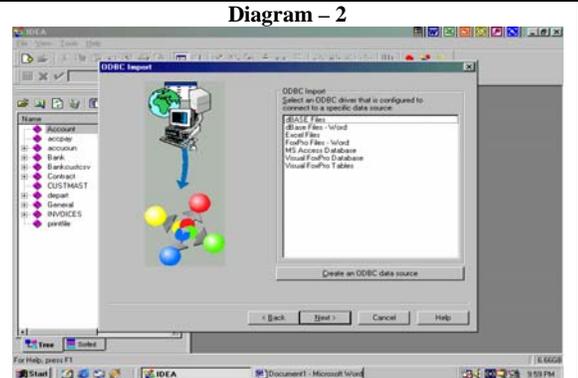


**10.23 Steps to import Oracle data into IDEA are given below:**

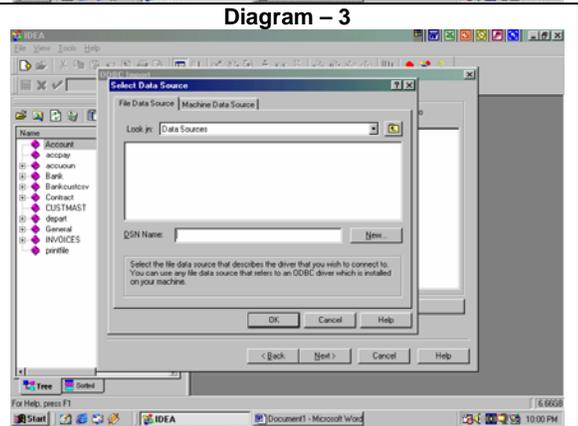
Ensure that the PC in use on which IDEA has been installed is connected to the auditees Data Base Server (in other words it allows you to Log on to their System).  
 Open the IDEA Software  
 Select the Import Assistant  
 Click on Use the ODBC to import the file option and press next as indicated in the **Diagram – 1**.



ODBC Import Box appears on the screen  
 A list of available ODBC Drivers is displayed in the Box as indicated in **Diagram – 2**.  
 Press on **Create an ODBC Data Source** button.



Clicking on Create on ODBC Data Source will open the screen as per **Diagram – 3**  
 Enter the **DSN** (Data Source Name) in the space provided.  
 Click on **OK**  
 If there is no connectivity between your pc and the Data Source Name, an error message will be displayed. Else it will take you to next screen as shown in **Diagram 4**.



Once the Screen as shown opposite is displayed, select the **Oracle ODBC Driver** option from the list of drivers

Press **Next**

If there is no connectivity, this will return an error message **“unable to access file”**.

Else this prompts you to the next screen as per **Diagram 5**.

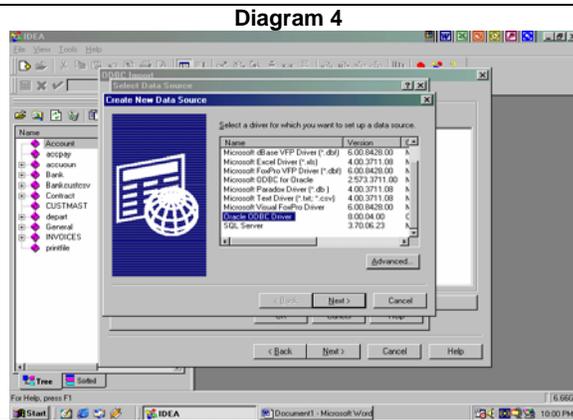


Diagram 4

The **Diagram 5** asks you to enter the file data source you want to save this connection to, Or, you can customize the location by clicking the browse button.

Press **Next**



Diagram 5

This will take us to the next screen as shown in **Diagram 6**.

Create New Data Source box appears and indicates the details of File Data Source (Filename and Driver name)

Press **Finish** button.

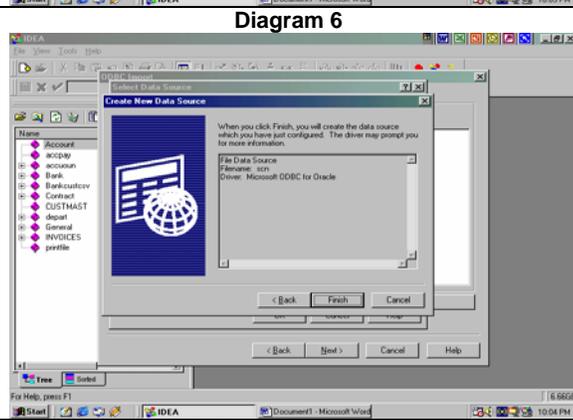


Diagram 6

Enter the User Name, Password and the Server Name in the **Microsoft ODBC for Oracle Connect** box.

(Note: the **User Name**, **Password** and **Server Name** to make use of the auditees database while Importing the tables into IDEA is to be obtained from the DBA of the Auditee organization)

Pressing the **OK** button will end the process of creation of an ODBC Data Source. In subsequent steps this created data source will be utilized for importing ORACLE Data Table in to IDEA.

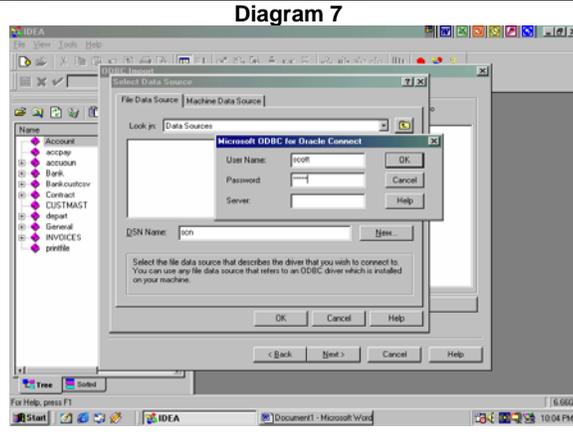


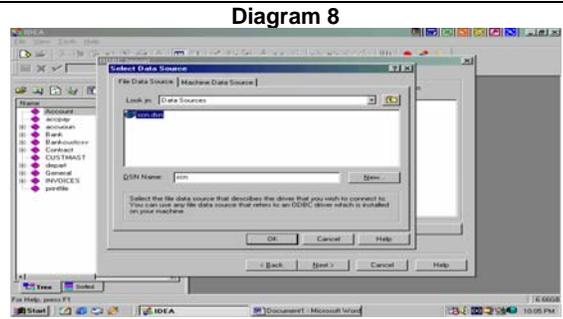
Diagram 7

Once the creation of ODBC Data Source is done this can be used any number of times for Importing the ORACLE Data Tables from the same server. For this:

Open the **Select Data Source** screen (Diagram 8).

This will show the name of **DSN name** created by us.

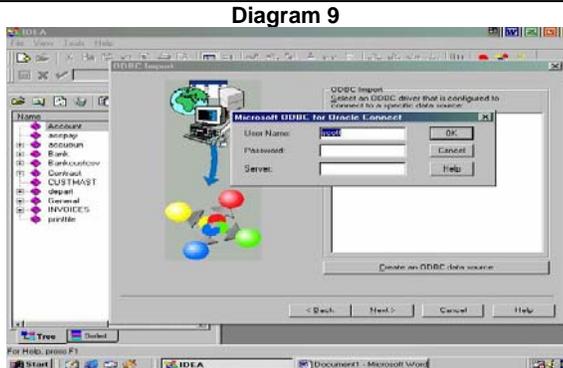
Select the created DSN name and press **OK**.



This will open the **Microsoft ODBC for ORACLE Connect** box (Diagram 9).

Enter the **User Name**, **Password** and the **Server Name**

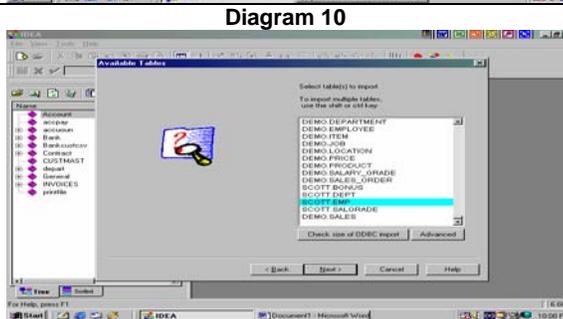
Press **OK**



Next screen (Diagram 10) will list the **Available Tables** in the auditee server as shown in Diagram 10. **Select the desired table(s)**.

The button **Check Size of ODBC Import** will ascertain the disk space required for importing the selected table(s).

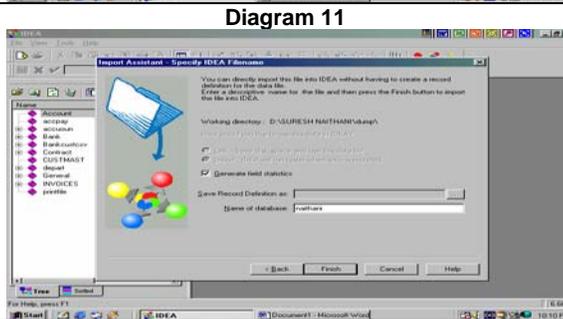
Press **Next** button.



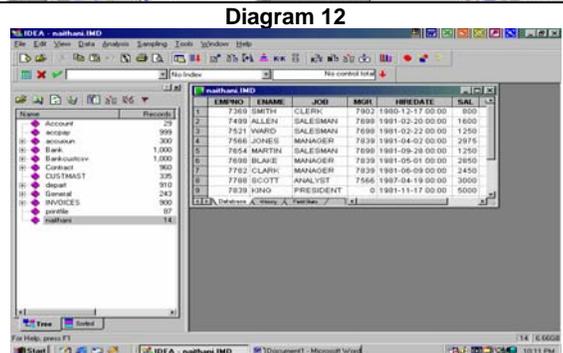
This brings us to the last screen (**Import Assistant – Specify Idea Filename**) of importing the table.

Enter the Idea file name for the imported table in the **Name of Database**

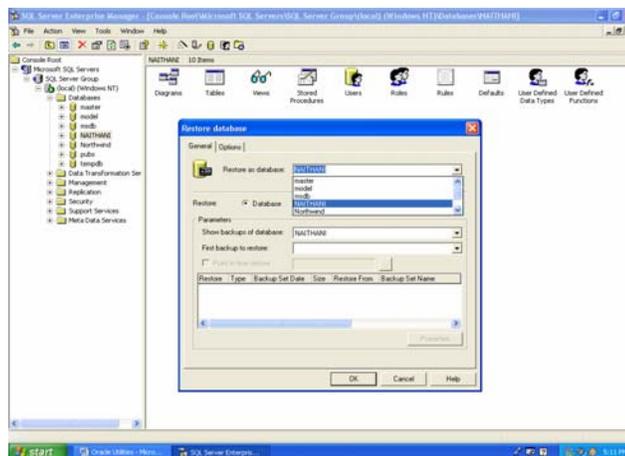
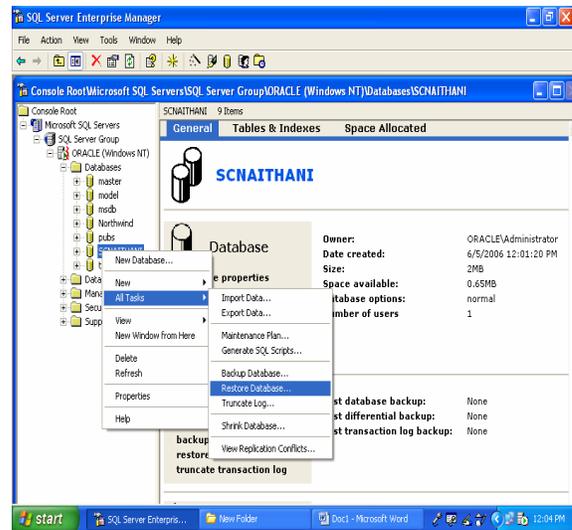
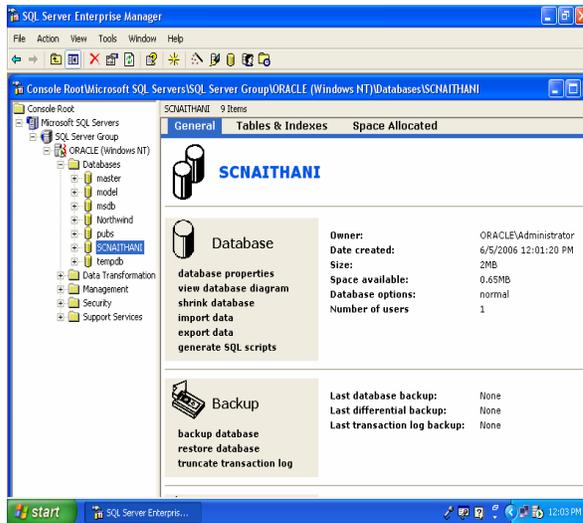
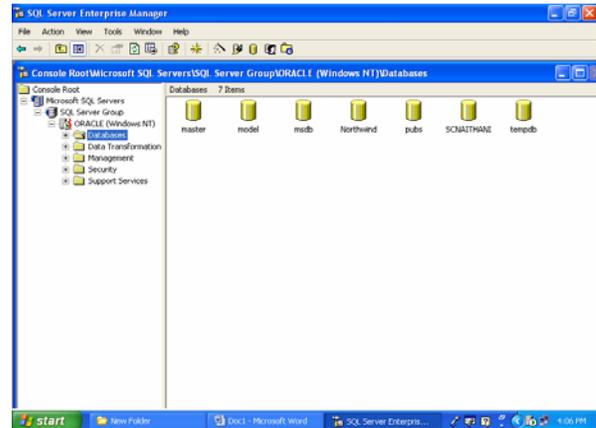
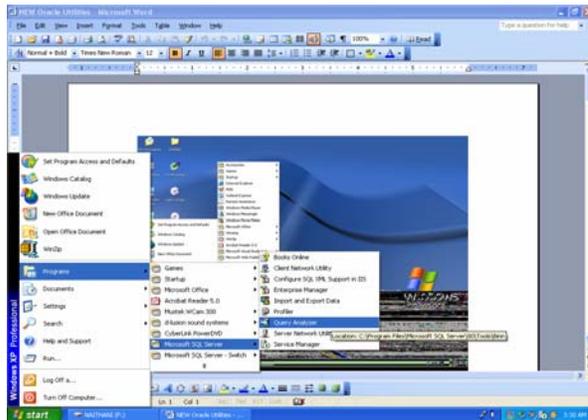
Press **Finish**



After importing the table, the imported table(s) can be used as other IDEA files. Analysis, Extractions, Sampling Techniques can be made use of. The imported table will appear like one shown in the **Diagram 12**.

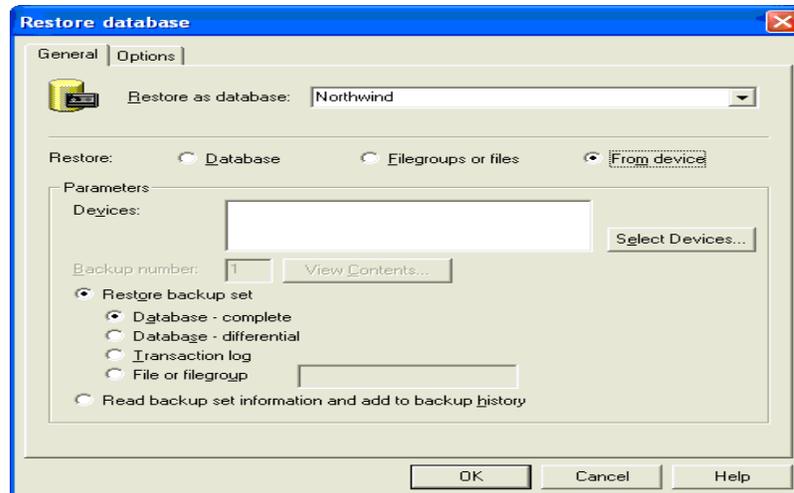


## 10.24 RESTORE SQL SERVER DATA BACKUP



In Enterprise Manager, right click on the database and select All Tasks. You will have options to Backup and Restore a database.

If you are not restoring on the same server, you can select the "From Device" option and find the files you want to restore. The screen will look like this.



Enterprise Manager: Restore database General tab

**Parameters:**

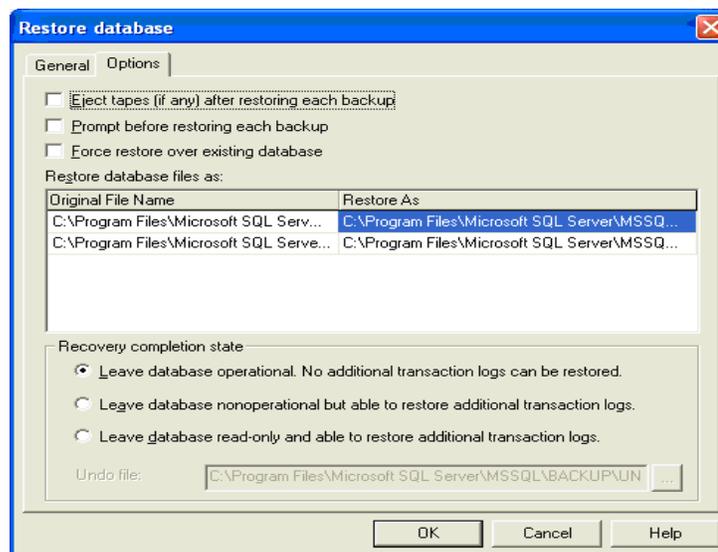
**Select Devices:** This button allows you to select the physical files you want to restore.

*Tip:* You can select multiple files to restore; sometimes you may have to restore each file individually and use the settings on the “Options” tab.

**Restore backup set:** You must select the corresponding option to the type of restore you are doing. So, if you are restoring a transaction log backup, you need to select Transaction Log.

**Read backup set information and add to backup history:** This option just reads the header information from the backup files and adds to the system tables in the msdb database.

For additional restore options, click the Options tab and this window appears:



Enterprise Manager: Restore database Options tab

**Eject tape (if any) after restoring each backup:** This is used if you are restoring from tape. Selecting this even though you are not using tapes won’t cause any problems.

**Prompt before restoring each backup:** A prompt window will pop up to let you know the restore has finished and asks if you want to restore the next file.

*Tip:* If you select cancel, it will leave the database in a “Loading” state, which means the restore process was not completed. To fix this, you can just rerun the restore process.

**Force restore over existing database:** If you are restoring backups and you want to overwrite an existing database with a different name, you must use this option. If you are restoring backups to the same database, this option is not required.

**Restore database file as:** This displays the name and location of the physical files used when you restore your database. The location and names of the files are stored in the backup file, so if you are restoring to a different server or to a different database name, you must change these options for both the data file and the transaction log file.

**Recovery completion state:**

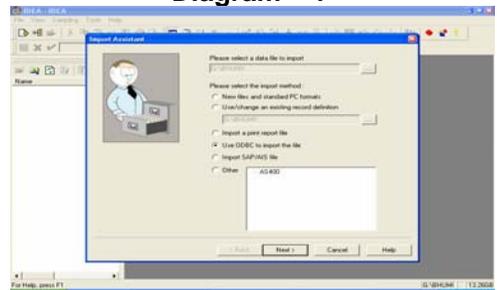
**Leave database operational:** This is the default option. After you restore your backups, the database is in a useable state and you cannot restore any additional backups.

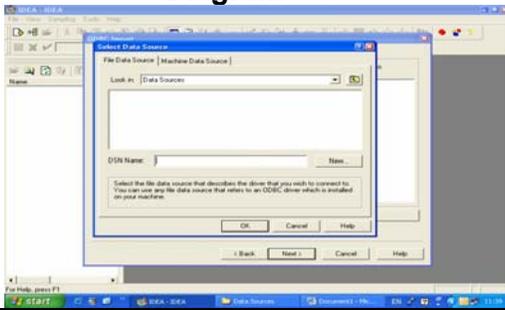
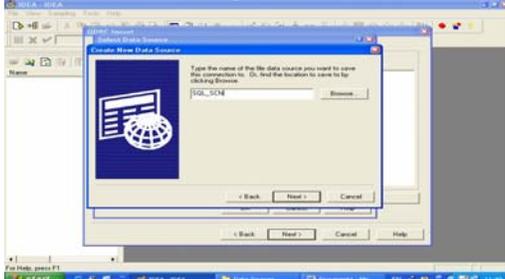
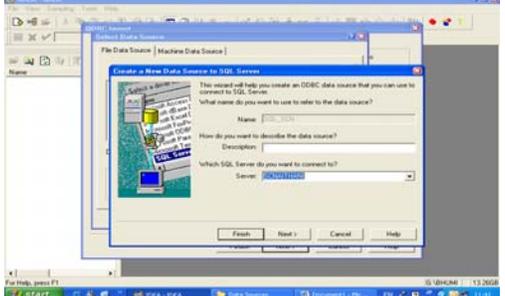
**Leave database nonoperational, but able to restore additional transaction logs:** This option allows you to restore a differential backup or additional transaction log backups. It will leave the database in a “Loading” state until the last restore is issued with the RECOVERY option or the first option above.

**Leave database read-only and able to restore additional transaction logs:** This option allows you to use the database in a read-only mode, but also allows you to restore additional transaction logs. This could be used for a reporting environment where you get transaction log backups from your production server and restore them to a different server on a set basis for read-only purposes.

**Undo file:** The undo file is used to undo uncommitted transactions when the database is brought fully online. If the undo file does not exist, it will be automatically created.

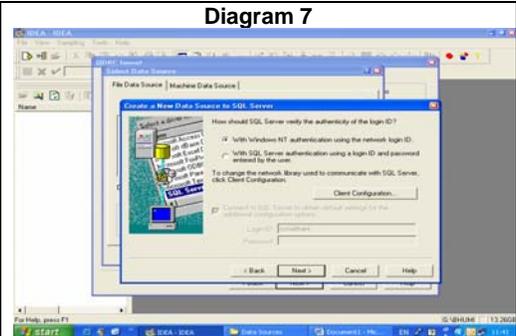
*10.25 Create SQL ODBC Driver*

<p>Select the Import Assistant</p> <p>Click on Use the ODBC to import the file option and press next as indicated in the <b>Diagram – 1</b>. Ensure that the PC in use on which IDEA has been installed is connected to the auditees Data Base Server (in other words it allows you to Log on to their System).</p> <p>Open the IDEA Software</p> <p>Select the Import Assistant</p> <p>Click on Use the ODBC to import the file option and press next as indicated in the <b>Diagram – 1</b>.</p>	<p style="text-align: center;"><b>Diagram – 1</b></p> 
<p>ODBC Import Box appears on the screen</p> <p>A list of available ODBC Drivers is displayed in the Box as indicated in <b>Diagram – 2</b>.</p> <p>Press on <b>Create an ODBC Data Source</b> button.</p>	<p style="text-align: center;"><b>Diagram – 2</b></p>

<p>Clicking on Create on ODBC Data Source will open the screen as per <b>Diagram – 3</b></p> <p>On DSN Name <b>Click New</b></p> <p>It will take you to next screen as shown in <b>Diagram 4</b>.</p>	<p style="text-align: center;"><b>Diagram – 3</b></p> 
<p>Once the Screen as shown opposite is displayed, select the <b>SQL Server</b> option from the list of drivers</p> <p>Press <b>Next</b></p>	<p style="text-align: center;"><b>Diagram – 4</b></p> 
<p>Diagram 5 asks you to enter the file data source you want to save this connection. Enter <b>New Name</b></p> <p><b>Click Next</b></p>	<p style="text-align: center;"><b>Diagram 5</b></p> 
<p>This will take us to the next screen as shown in <b>Diagram 6</b>.</p> <p>Create New Data Source box appears and indicates the details of File Data Source (Filename and Driver name)</p> <p>Press <b>Finish</b> button.</p>	<p style="text-align: center;"><b>Diagram 6</b></p> 
<p>This will ask you to “Which SQL Server do you want to connect to ?” as shown in <b>Diagram 6</b>.</p> <p>Enter the SQL Server Name e.g. <b>SCNAITHANI</b> in Diagram 6</p> <p>Instead of pressing finish select the <b>Next</b> option to <b>choose the Database</b></p> <p><b>Click Next.</b></p>	<p style="text-align: center;"><b>Diagram 6</b></p> 

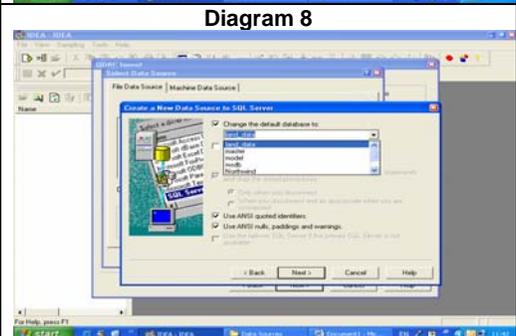
Now SQL Server will verify the authenticity of the User by asking for login ID. By default it will select the option of Windows NT authentication using.

Click Next

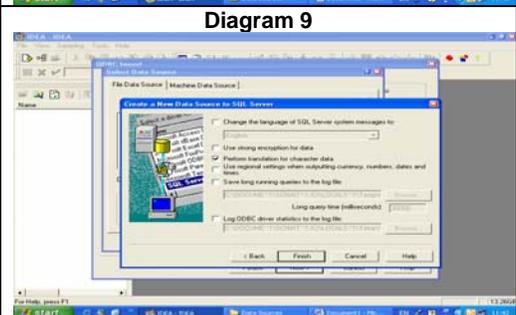


This screen allows to select the desired Database by pressing dropdown list.

Click Next

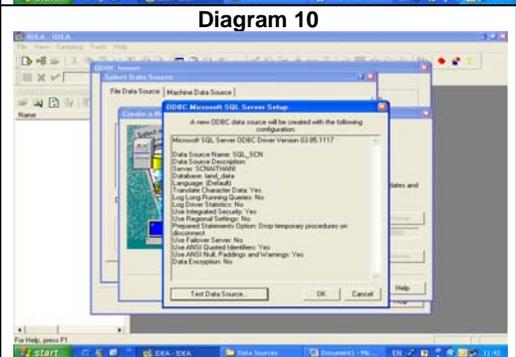


Press Finish for Next



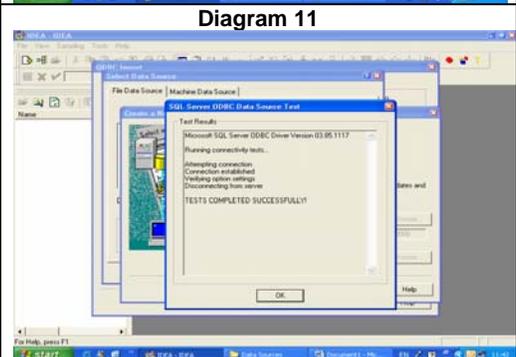
After pressing this will give the detail of new ODBC data source created by the user as shown in Diagram 10.

Click Test



If test is completed successfully, screen as per Diagram 11 will be displayed

Click OK





**Contributors to the IT Audit Manual :**

Subhashini Srinivasan

Vani Sriram CISA, CIA

Rajesh K Goel CISA, CIA

G Srinivas CISA, CIA

Dr Ashutosh Sharma CISA

**IT Audit Manual peer reviewed by**

Anupam Kulshreshtha CISA, CISM, CIA

N Nagarajan CISA, CISM, CIA

Subir Mallick

A K Ojha CISA

**IT Audit Manual preparation support Group**

Namashivayam CISA

K P Singh

Murali Krishnan

B J Chanda

S C Naithani