Annexure-10
(referred to in Para 5.1.2)

COBIT framework

- COBIT (Control Objectives for Information and related Technology) was first released by the Information Systems Audit and Control Foundation (ISACF) in 1996. Since then COBIT has been enhanced with existing and emerging international technical, professional, regulatory and industry-specific standards.

- COBIT helps meet the multiple needs of Management by bridging the gap between business risks, control needs and technical issues.

- Business orientation is the main theme of COBIT. It is designed to be employed not only by users and auditors, but also as comprehensive guidance for Management and business process owners.

- The control objectives make a clear and distinct link to business objectives and are defined in a process-oriented manner following the principle of business re-engineering. At identified domains and processes a high level control objective is identified and rationale provided to document the link to the business objectives. In addition, considerations and guidelines are provided to define and implement the IT control objective.

- The classification of domains where high level control objectives apply (domains and processes), an indication of the business requirements for information in that domain as well as the IT resources primarily impacted by control objectives, together form the COBIT framework. The framework has identified 34 High-Level Control Objectives and 318 Detailed Control Objectives.

Methodology of Audit under COBIT

- In an organisation there are three levels of IT efforts in the management of IT resources.

- Starting at the bottom are the Activities and Tasks needed to achieve a measurable result. Activities have a lifecycle concept while tasks are more discrete. The lifecycle concept has typical control requirements different from discrete activities.

- Processes are then defined one layer up as a series of joined activities or tasks with natural control breaks.

- At the highest level, processes are naturally grouped together into Domains. Their natural grouping is often confirmed as responsibility domains in an organisational structure and is in line with the management cycle or lifecycle applicable to IT processes.

Thus, the conceptual framework can be approached from three vantage points.

The Framework's Principles

Business Requirements

IT Processes

IT Resources
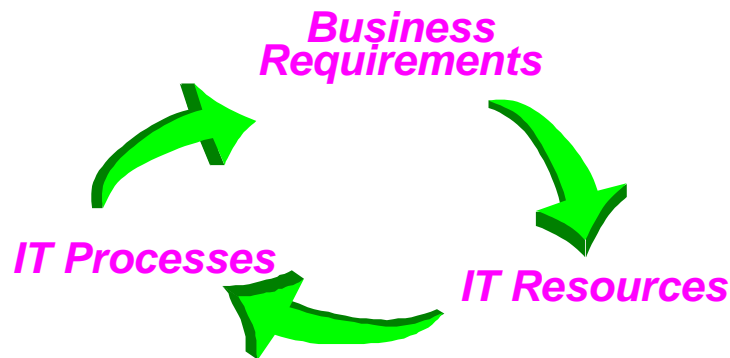
(i) Business Requirements are classified into Quality (Quality, Cost and Delivery), Fiduciary (Effectiveness and efficiency, Reliability of information and Compliance of laws and regulations) and Security (Confidentiality, Integrity and Availability);

(ii) IT Resources consist of People, Application, System, Technology, Facilities and Data;

(iii) IT Processes are divided into Domains, Processes and Activities.

- To satisfy business objectives, information needs to conform to certain criteria, which COBIT refers to as business requirements. These are Quality, Effectiveness, Efficiency, Confidentiality, Integrity, Availability, Compliance and Reliability

In a System Development and Management four broad Domains are identified

(i)   Planning and organisation**:** This domains covers strategy and tactics and concerns the identification of the way IT can best contribute to the achievement of business objectives.

(ii)   Acquisition and implementation: To realise the IT strategy, IT solutions need to be identified, developed or acquired as well as implemented and integrated into business process.

(iii)   Delivery and Support**:** This domain is connected with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training.

(iv)   <u>Monitoring</u>: All IT processes need to be regularly assessed over time for their quality and compliance with control requirements.

All the control measures will not necessarily satisfy the different business requirements for information to the same degree. Various degrees are as follows**:**

➢   Primary is the degree to which the defined control objectives directly impact the information criterion concerned.

➢   Secondary is the degree to which the defined control objectives satisfy only to a lesser extent or indirectly the information criterion concerned.

➢   Blank could be applicable. However, requirements are more appropriately satisfied by another criterion in this process and/or by another process.

• The control over an IT process and its activities with specific business goals ensures delivery of information to the business that addresses whether the required information criteria are measured by Key Goal Indicators. It is enabled by creating and maintaining a system of process excellence and control appropriate for the business. It considers Critical Success Factors that leverage specific IT Resources and are measured by Key Performance Indicators.

Key Goal Indicators as defined are:

• Increased level of service delivery;
• Availability of systems and services;
• Cost efficiency of processes and operations;
• Confirmation of reliability and effectiveness;
• Staff productivity and morale.

Critical Success Factors are:

• IT performance is measured in financial terms, in relation to customer satisfaction, for process effectiveness and for future capability and IT management is rewarded based on these measures;

• The processes are aligned with the IT strategy and with the business goals; they are scalable and their resources are appropriately managed and leveraged;

• A business culture is established, encouraging cross-divisional co-operation and teamwork, as well as continuous process improvement;

• Goals and objectives are communicated across all disciplines and are understood;

• A continuous process quality improvement effort is applied;

• The required quality of staff (training, transfer of information, morale, etc.) and availability of skills exist (recruit, retain, re-train).

Key Performance Indicators are:

- ✓ System downtime;
- ✓ Throughput and response times;
- ✓ Amount of errors and rework;
- ✓ Number of staff trained in new technology and customer service skills;
- ✓ Benchmark comparisons;
- ✓ Number of non-compliance reporting;
- ✓ Reduction in development and processing time.

- COBIT provides Maturity Model for control over IT processes, so that the Management can map where the organisation is today, where it stands in relation to the best-in-class in its industry and to international standards and where the organisation wants to be (refer to Annexure 11).

Annexure-11
(referred to in para 5.1.2)

Generic Process Maturity Model

- **Non- Existent:** Complete lack of recognisable processes**.**

- **Initial/Ad hoc:** There is evidence that the organisation has recognised that the issues exist and need to be addressed. There are, however, no standardised processes but instead there are ad hoc approaches.

- **Repeatable but Intuitive:** Processes have been developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures and responsibility is left to the individual.

- **Defined Process:** Procedures have been standardised and documented and communicated through training. It is, however, left to the individual to follow these processes.

- **Managed and Measurable:** It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively.

- **Optimised:** Processes have been refined to a level of best practice. IT is used in an integrated way to automate the workflow. Providing tools to improve quality and effectiveness, making the enterprise quick to adopt.

Annexure-12
(referred to in Para 5.1.2)

**Audit Methodology for project-manthan**

The special features of the Audit Methodology followed in the Performance Audit of Information Technology (IT) Re- engineering Project (Manthan) are given below:

• Performance Audit has been conducted of an ongoing IT Project of substantial investment outlay of approximately Rs.300 crore.

• The Project is complex and is characterised by the involvement of multiple third parties including consultants, software and hardware suppliers, maintenance contractors and the Department of Telecommunications.

• Performance Audit has been conducted in conformity with the methodology as enunciated in the COBIT framework.

• Performance Audit has been conducted of an ongoing IT Project thereby reviewing the emerging transitional changes in Systems Development Implementation upto June 2004.with an evaluation of the IT System and with an emphasis on IT Governance, an increasingly significant concept, that is essential for the success of Enterprise Governance♣ as it integrates and institutionalises the best practices of Planning and Organising, Acquiring and Implementing, Delivering and Supporting and Monitoring IT performance , with a view to ensuring that the information and technology in the enterprise, support its business objectives.

• Accordingly, Audit had to orient its approach duly focusing on ascertaining whether the enterprise was in a position to optimise and obtain full advantage of its information, thereby maximising benefits, capitalising on opportunities and consequently gaining competitive advantage.

• With a view to ensuring the commencement and timely completion of Performance Audit within a pre-determined timeframe and with due regard to ensuring and facilitating the process of a proper appreciation and understanding of the COBIT Framework and its various components by the Corporate Management Audit ensured the following:

(i)   a system of regular inter-action between the Audit Team and the Management;

(ii)   emphasising the need for swift responses from the Management to Audit Observations;

♣*Enterprise Governance has been holistically defined as " the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organisation's resources are used responsibly" (Information Systems Audit and Control Foundation, 2001.*

(iii) emphasising the need for providing the requisite documentation for substantiation of the Management replies furnished through interviews, replies to Audit memoranda and questionnaires;

(iv) Presentations were made to the Senior Management of the organisation regarding the methodology proposed for adoption while conducting the Audit. It included a detailed coverage of the following:

- An Executive Summary;

- The Framework of Domains, Processes and Control Objectives covering 34 High-Level Control Objectives and 318 Detailed Control Objectives;

- Management Guidelines;

- Audit Guidelines;

- The concepts of Maturity Model, Critical Success Factors, Key Goal Indicators.
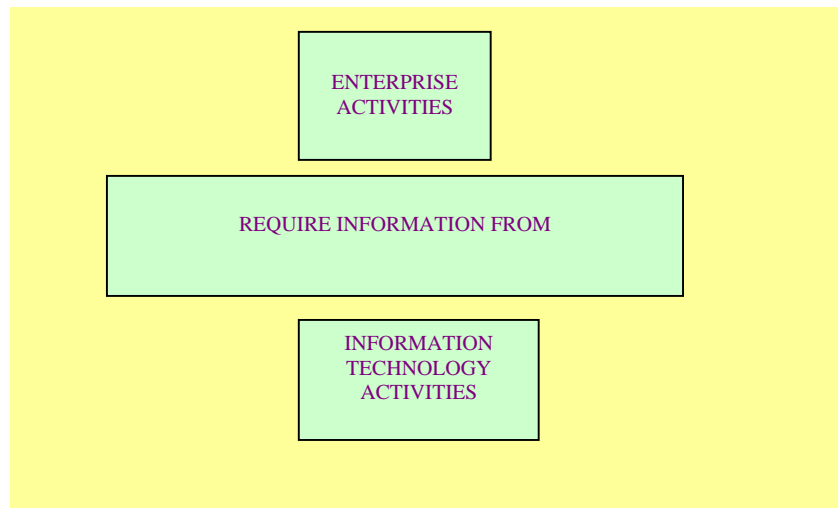
A presentation was, in turn, made by the Electronics Data Processing Management regarding the highlights and salient features of the ERP Project Manthan. These meetings provided an effective platform for Audit and Management interface and, thus, facilitated the process of understanding the entity and its environment, both prior to the commencement of implementation of the Project and thereafter.

Other significant features of the Methodology included:

- Preparation and issue of detailed questionnaires for each of the four Domains (395 in all) under COBIT, for ensuring clear and comprehensible components for facilitating the receipt of responses from the Management.

- Structured interviews and collection of Audit evidence through Questionnaires and Check lists. More than 35 Structured interviews/ Meetings with a coverage of more than 100 officers were held at various levels, followed up by a process of collection of documentation.

- 25 out of 99 pilot sites were visited by the Audit Team for on-site evaluation of the IT System and collection of Audit Evidence. In addition offices of Members Audit Board of other regions gave the material for nine sites.

- Management confirmation of Minutes of Meetings held and continuous interaction at all levels with Management of the audited entity during the period.

- The following documents were examined in detail:

- Deliverables issued by the Consultants (Deliverables-1 to 14);
- Installation Manual;
- Operations Manual;
- Security and Authorisation–Roles and Transactions;
- SAP Testing Strategy;
- System Landscape and Hardware Sizing Document, Testing, Country India Reference and Info Data Base Servers;
- Proposed Codification Structure for Company's Chart of Accounts;
- Disaster Recovery Guide for Data Centre and Emergency Procedure;
  The Consultant designed the above documents.

In addition to the above the following documents were also reviewed during the Performance Audit:-

- Documents relating to the Selection Procedure of ERP vendors;
- Copies of Purchase Orders and Agreements with ERP vendors and the Consultants;
- Purchase Orders–Annual Maintenance Contracts;
- General Conditions of Contract;
- Personnel Manual;
- Administration Manual.

Annexure-13
(referred to in Para 5.1.1)

Enterprise Resource Planning (ERP)

(i) Enterprise Resource Planning system is a packaged business software system that enables an organisation to manage and synergise the efficient and effective use of its resources:
- Materials,
- People,
- Machinery, Plant and Equipment.

It integrates all facts of business operations.

(ii) Important attributes of ERP are its ability to:

- Automate and integrate the majority of an organisation's business processes;
- Share common data and practices across the entire organisation;
- Produce, access and analyse information flows in a real-time environment that would support decision-making at all levels by providing the required information to the right people at the right time and in the proper format;
- Elimination of redundant data and procedural operations;
- Flexibility to allow for customisation;
- Compulsive use of best practices because of software;
- Increased efficiency hence reduced costs;
- Adaptability to a changing business environment;
- Reduced cycle times;
- Functional interaction among various modules.

(iii)   Precautions necessary for successful implementation of an ERP system include:

- Effective cost control mechanisms due to large investment outlays as rapid implementation would result in shortened ROI (Return on Investment) periods;
- Avoidance of mismatches between the proposed model, the ERP functionality and the customisation process so as to ensure avoidance of extended implementation time-frames, higher costs and the loss of user confidence;
- Adherence to a well-planned and realistically assessed and structured time schedule for implementation and commissioning;
- Effective vendor management.

    Ensuring effective integration and interface with the surviving legacy systems.

Annexure-14

(referred to in Para 5.1.6)

Statement showing the target and actual date of implementation of ERP software SAP/R3

Description	Proposed date of start Actual date of start	Initial target date of completion Revised target date of completion	Actual date of completion	Delay in months with reference to the revised target dates.
Stage-I Conceptualisation and design	April 1997	October 1997	July 1998	seven months
	July 1997	December 1997		
Selection of ERP Software/vendor and diversion of the scope of work of Consultants	---	---	September 1999. The Company paid Rs 33.27 lakh to Consultants for SAP selection	--
	July 1998	----		
Stage-II Development, Testing and Implementation of SAP at 99 sites	August 1998	September 1999	October 2003	12 months
	October 1999	36 Months (as per revised Targets) October 2002		
Roll out beyond 99 sites (Implementation of SAP at 429 sites)	October 1999	September 2002	November 2004	11 months
	November 2003	December 2003		
Delay in the implementation of Supply Chain Management System (add- ons)				
Supply Chain Management system (Phase-I)	June 2001	April 2002	September 2004	seven months
	October 2002	16 months February 2004		
Supply Chain Management System (Phase-II) including integration with ERP.	December 2001	April 2002	---	----
	October 2004	September 2005		