SYSTEM: A set of interrelated elements that operate collectively to accomplish some common purpose or goal.	**TYPES OF SYSTEM** 1. Elements: • Abstract system • Physical system 2. Interactive Behaviour: • Closed system • Open system • Entropy 3. Degree of Human Intervention: • Manual system • Automated system 4. Working/Output – • Deterministic system • Probabilistic system	**GENERAL MODEL OF A SYSTEM:** A general model of a physical system is input, process and output. This is, of course, very simplified because a system may have several inputs and outputs. • Input • Processing • Output • Storage • Feedback	**SYSTEM ENVIRONMENT** • **Boundary:** The features that define and delineate a system form its boundary. • **Sybsystem:** A subsystem is a part of a larger system. • **Interfaces:** The inter connections & interactions between the subsystem are termed interfaces.
CHARACTERISTICS OF SUBSYSTEMS: Decomposition Simplification Decoupling	**INFORMATION:** Information is data that has been processed into a form that is meaningful to the recipient and is of real or perceived value in current or progressive decision.	**CHARACTERISTICS OF INFORMATION: (CAR has MRF Tyres and Voice Recorder)** • Completeness • Cost Benefit Analysis • Accuracy and Quality • Relevance and Purpose • Mode and Format • Redundancy • Frequency • Timleliness • Validity • Reliability	**TYPES OF INFORMATION:** • Internal information • External information

INFORMATION SYSTEM AND ITS ROLE IN MANAGEMENT: An information system can be considered as an arrangement of a number of elements that provides effective information for decision-making and/or control of some functionalities of an organisation: Implications: • Decision-making • Competitive edge • Innovative ideas • Knowledge • Formulate a strategy	**FACTORS ON WHICH INFORMATION REQUIREMENTS DEPEND:** Operational function Type of decision making: • Programmed decisions or structured decisions • Non-programmed or unstructured decisions Level of management activity: • Strategic Level or Top Level • Tactical Level or Middle Level • Supervisory or Operational Level	**COMPONENTS OF COMPUTER BASED INFORMATION SYSTEM** A Computer-based Information System (CBIS) is an information system in which the computer plays a major role. Such a system consists of the following elements: • Hardware • Software • Data • Procedures • People	**OPERATIONS SUPPORT SYSTEMS (OSS)** • Transaction Processing Systems – TPS • Management Information Systems – MIS • Enterprise Resource Planning Systems – ERP
TRANSACTION PROCESSING SYSTEM (TPS): It involves • Capturing data • Processing of files/databases • Generating information • Handling of queries	**TPS COMPONENTS** • Inputs • Processing • Storage • Outputs	**FEATURES OF TPS** • Large volume of data • Automation of basic operations • Benefits are easily measurable • Source of input for other systems	

<table>
<tr>
<td>MANAGEMENT INFORMATION SYSTEM (MIS): An integrated user-machine system designed for providing information to support operational control, management control and decision making functions in an organisation.</td>
<td>CHARACTERISTICS OF AN EFFECTIVE MIS:
(MICS is a History)
• Management Oriented
• Management Directed
• Integrated
• Common Database
• Computerised
• Sub system concept
• Heavy Planning Element</td>
<td>MISCONCEPTIONS OR MYTHS ABOUT MIS:
• The study of management information system is about the use of computers.
• More data in reports means more information for managers.
• Accuracy in reporting is of vital importance.</td>
<td>PRE-REQUISITES OF AN MIS: (D – CESS)
• Database
• Control and Maintenance of MIS
• Evaluation of MIS
• System and Management Staff should be qualified
• Support of Top Management</td>
</tr>
<tr>
<td>CONSTRAINS IN OPERATING A MIS: (QUEST)
• Qualified staff not available
• Quantifying the benefits of MIS is difficult
• Expert's turnover is high
• Selection of sub system of MIS
• Standardised approach not possible
• Staff's Cooperation not available</td>
<td>EFFECTS OF USING COMPUTER IN MIS: (ISCA)
• Increases the effectiveness of Information Systems
• Integrates the working of different information subsystem
• Speed of processing and retrieval of data increases
• Scope of use of information system has expanded
• Complexity of system design & operation increased
• Comprehensive information
• Analysis widens</td>
<td colspan="2">LIMITATIONS OF MIS: (LIMITATION)
• Less useful for unstructured data
• Internal information is taken into consideration
• Management keeps changing so does their goals
• Inputs and processing quality determines the quality of outputs
• TPS's limitations still exists in MIS
• Ad-hoc reporting is not possible
• The attitudes and moral are ignored in MIS
• Integration is lacking
• Hoarding of information reduces the effectiveness
• Not a substitute for effective management</td>
</tr>
</table>

ENTERPRISE RESOURCE PLANNING (ERP) SYSTEMS: • ERP system is a fully integrated business management system • It organizes and integrates – operation processes and information flows, to make optimum use of resources • ERP aims at one database, one application, and one user interface	**OBJECTIVES:** • Provide support for adopting best business practices • Implement these practices with a view towards enhancing productivity • Empower the customers and suppliers to modify the implemented business processes to suit their needs	**AN ERP SYSTEM INTEGRATES VARIOUS BUSINESS PROCESSES:** • Business System • Production • Maintenance • Quality Control • Marketing • Finance • Personnel • Consolidation of Business Operations	**MYTHS OF ERP SYSTEM:** • There is a misconception that ERP is a computer system. • There is a misconception that ERP is relevant for manufacturing organisations only.
BENEFITS OF ERP: • Better use of organisational resources • Lower operating costs • Proactive decision making • Enhanced customer satisfaction • Flexibility in business operations	**LIMITATIONS OF ERP:** • An ERP system provides current status only • The methods used in the ERP applications are not integrated with other organisational or divisional systems.	**MANAGEMENT SUPPORT SYSTEMS (MSS):** Focus on the managerial uses of information resources and provide information to managers for planning and decision making. There are three types of MSS, namely: • Decision Support Systems (DSS) • Executive Information (Support) System (EIS) • Expert Systems	

DECISION SUPPORT SYSTEMS (DSS): is a system that provides tools to managers to assist them in solving semi structured and unstructured problems in their own, somewhat personalized, way.	**CHARACTERISTICS OF DSS: (SEA)** • Support semi-structured/Unstructured decision making • Ease of learning and use • Ability to adapt to changing need	**COMPONENTS OF A DSS:** • The User: - Manager - Staff Specialist (Analysts) • Databases: - Physical Level - Logical Level - External Level • A planning language • Model Base
EXECUTIVE INFORMATION SYSTEMS (EIS): It is a tool that is designed to meet the special needs of top-level managers. It provides direct on-line access to relevant information in a useful and navigable format.	**EXECUTIVE ROLES AND DECISION MAKING:** • Strategic Planning • Tactical Planning • Fire Fighting • Control	**PRINCIPLES TO BE FOLLOWED WHILE DESIGNING AN EIS:** EIS must be: • Easy to understand and collect • Based on a balanced view of the organisation's objectives • Reflecting everyone's contribution in a fair and consistent way • Encouraging for the management and staff • Available to everyone in the organisation • Evolving to meet the changing needs of the organisation

EXPERT SYSTEMS Expert Systems are software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such expert systems.	**NEED FOR EXPERT SYSTEMS** • Expert labour is expensive and scarce. • No matter how bright or knowledgeable certain people are, they often can handle only a few factors at a time.	**BENEFITS OF EXPERT SYSTEMS** • preserve knowledge • put information into an active-form • assist novices in thinking the way experienced professional do. • not subject to such human fallings as fatigue, being too busy, or being emotional. • can be effectively used as a strategic tool is the areas of marketing products, cutting costs and improving products.	**THE PROPERTIES THAT POTENTIAL APPLICATIONS SHOULD POSSESS TO QUALIFY FOR EXPERT SYSTEM DEVELOPMENT ARE:** • Availability • Complexity • Domain • Expertise • Structure
COMPONENTS OF EXPERT SYSTEMS • Knowledge Base (KB) • Inference Engine - forward-chaining mechanism - backward chaining mechanism • Knowledge Acquisition Subsystem (KAS) • User Interface	**OFFICE AUTOMATION SYSTEMS (OAS):** is the application of computers to handle the office activities: • Document Capture • Document Creation • Receipts and Distribution • Filling, Search, Retrieval and Follow up • Calculations • Recording Utilisation of Resources	**BENEFITS OF OFFICE AUTOMATION SYSTEMS** • Improve communication • Reduce the cycle time between preparation and receipt of messages • Reduce the costs of office communication • Ensure accuracy of communication flows	**CATEGORIES OF COMPUTER BASED OFFICE AUTOMATION SYSTEMS:** • Text Processing Systems • Electronic Document Management Systems • Electronic Message Communication Systems • Teleconferencing and Video-conferencing Systems

---****---

SYSTEMS DEVELOPMENT PROCESS:
Systems development refers to the process of examining a business situation with the intent of improving it through better procedures and methods.

- System Analysis
- System Design

REASONS FOR FAILURE:

- Lack of senior management support for and involvement in information systems development
- Shifting user needs
- Development of strategic systems
- New technologies
- Lack of standard project management and systems development methodologies
- Overworked or under-trained development staff
- Resistance to change
- Lack of user participation
- Inadequate testing and user training

THE CHARACTERISTICS OF SYSTEM DEVELOPMENT METHODOLOGY:

- The project is divided into a number of identifiable processes
- Deliverables must be produced
- Users, managers and auditors are required to participate in the project to provide sign-offs.
- The system must be tested thoroughly
- A training plan is developed
- Formal program change controls are established
- A post-implementation review of all developed systems must be performed

APPROACHES TO SYSTEM DEVELOPMENT

- Waterfall: Linear framework type
- Prototyping: Iterative framework type
- Incremental: Combination of linear and iterative framework type
- Spiral: Combination linear and iterative framework type
- Rapid Application Development (RAD): Iterative Framework Type
- Agile Methodologies

SYSTEM DEVELOPMENT LIFE CYCLE (SDLC): framework provides system designers and developers to follow a sequence of activities. It consists of a set of steps or phases in which each phase of the SDLC uses of results of the previous one.

THE PHASES INVOLVED IN THE SDLC: (I Require A Design Developer To Implement and Maintain)

- Preliminary Investigation
- Systems Requirements Analysis
- Systems Design
- Systems Acquisition & Development
- Systems Testing
- Systems Implementation
- Post Implementation Review and Maintenance

STAGE-I: PRELIMINARY INVESTIGATION – OBJECTIVES **Objective:** To determine and analyze the strategic benefits in implementing the system through evaluation and quantification of – productivity gains; future cost avoidance; cost savings and intangible benefits like improvement in morale of employees.	**1. IDENTIFICATION OF PROBLEM** • Clarify and understand the project request • Determine the size of the project • Determine the technical and operational feasibility of alternative approaches • Assess costs and benefits of alternative approaches • Report findings to the management with recommendation outlining the acceptance or rejection of the proposal **2. IDENTIFICATION OF OBJECTIVE** After the identification of the problem, it is easy to work out the objectives of the proposed solution.	**3. DELINEATION OF SCOPE** • Functionality requirements • Data to be processed • Control requirements • Performance requirements • Constraints • Interfaces • Reliability requirements **Methods with the help of which the scope of the project can be analyzed are as follows:** • Reviewing internal documents • Conducting interviews
4. FEASIBILITY STUDY: (LOBSTER Fry) • Legal • Operational • Behavioural • Schedule/Time • Technical • Economical • Resources • Financial	**ESTIMATING COST & BENEFIT** **COSTS:** • Development • Operational • Intangible **BENEFITS:** • Tangible • Intangible	

STAGE-II: SYSTEMS REQUIREMENTS ANALYSIS FACT FINDING TECHNIQUES (DIQO) Documents Interviews Questionnaires Observations	**ANALYSIS OF PRESENT SYSTEM** • Review Historical Aspects • Analyze Inputs • Review Data Files Maintained • Review Methods, Procedures & data Communications • Analyze Output • Review Internal Controls • Model the Existing Physical & Logical System • Undertake Overall Analysis	**SYSTEMS ANALYSIS OF PROPOSED SYSTEMS:** After each functional area of the present information system has been carefully analysed, the proposed system specifications must be clearly defined.
SYSTEM DEVELOPMENT TOOLS: 1. System Components & Flows • System Flow Chart (SFC) • Data Flow Diagram (DFD) - Data Source & destination - Data Flows - Transformation Process - Data Stores • System Components Matrix • CASE Tools 2. User Interface 3. Date Attributes & Relationship 4. Detailed System Process	**STRUCTURED ENGLISH:** Structured English, also known as Program Design Language (PDL) or Pseudo Code, is the use of the English language with the syntax of structured programming. Thus, Structured English aims at getting the benefits of both the programming logic and natural language. Program logic that helps to attain precision and natural language that helps in getting the convenience of spoken languages.	**FLOWCHARTS:** Flowcharting is a graphic technique that can be used by analysis to represent the inputs, outputs and processes of a business in a pictorial form. It is a common type of chart, that represents an algorithm or process showing the steps as boxes of various kinds, and their order by connecting these with arrows. Flowcharts are used in analyzing, designing, documenting or managing a process or program in various fields.

TYPES OF FLOW CHARTS • Document flowchart • Data flowchart • System flowchart • Program flowchart	**BENEFITS OF FLOWCHART:** • Communication • Effective analysis • Proper documentation • Efficient Coding • Proper Debugging • Efficient Program Maintenance	**LIMITATIONS OF USING FLOWCHARTS:** • Complex logic • Alterations and Modifications • Reproduction • The essentials of what is done can easily be lost in the technical details of how it is done.
DECISION TREE: A Decision Tree (or tree diagram) is a support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility. **DECISION TABLE:** A Decision Table is a table which may accompany a flowchart, defining the possible contingencies that may be considered within the program and the appropriate course of action for each contingency Condition Stub – which comprehensively lists the comparisons or conditions; • Condition Stub • Action Stub • Condition entries • Action entries	**DATA DICTIONARY:** It is a computer file that contains descriptive information about the data items in the files of a business information system. In other words, it is a computer file about data. **Uses:** • Aids in documentation – To programmers & analysis • File Security • For Accountant – Planning flow of transaction data • For Auditors – Establish audit trail • Aids in investigation/documenting internal control procedures	**Data Dictionary Contains:** • Data item's length, type & range • Identify of source document used to create data item • Names of computer file storing data item • Names of computer programs that modify data item • Identify of individual permitted to access • Identify of individual not permitted to access

LAYOUT FORM AND SCREEN GENERATOR, MENU GENERATOR, REPORT GENERATOR, CODE GENERATOR • Layout form and Screen Generator • Menu Generator • Report Generator • Code Generator	**SYSTEM SPECIFICATION** At the end of the analysis phase, the systems analyst prepares a document called "Systems Requirement Specifications (SRS)", it contains: • Introduction • Information Description • Functional Description • Behavioural Description • Validation Criteria • Appendix • SRS Review	**ROLES INVOLVED IN SDLC** • Steering Committee • Project Manager • Project Leader • Systems Analyst/Business Analyst • Module Leader/Team Leader • Programmer/Coder/Developer • Database Administrator (DBA) • Quality Assurance • Tester • Domain Specialist • IS Auditor
STAGE – III: SYSTEM DESIGN System design involves first logical design and then physical construction of a system. Design specifications instruct programmers about what the system should do. The programmers, in turn, write the programs that accept input from users, process data, produce the reports, and store data in the files.	**THE DESIGN PHASE INVOLVES:** • Architectural Design • Design of the Data/Information Flow • Design of the Database • Design of the User-interface • Physical Design • Design and acquisition of the hardware/system software platform	**DESIGN OF DATABASE** • Conceptual Modeling • Data Modeling • Storage Structure Design • Physical Layout Design

DESIGN OF USER-INTERFACE **Output Objectives:** • Convey info about past, current, future • Signal important events, opportunities, warnings • Trigger an action • Confirmation of action • Meets needs of organisation & users	**Important factors in Input/Output design: (CM's Fraud on TV)** • Content • Media • Form • Format • Timeliness • Volume	**PHYSICAL DESIGN:** **Design Principles-** • The recommended procedure is to design two or three alternatives & choose the best one on pre-specified criteria. • The design should be based on the analysis. • The software functions designed should be directly relevant to business activities. • The design should follow standards laid down. • The design should be modular.
Stage – IV – Part 1: SYSTEM ACQUISITION **Acquisition Standards** • Ensuring security, reliability and functionality already built into a product. • Ensuring managers complete appropriate vendor, contract, and licensing reviews. • Including invitations-to-tender and request-for-proposals. • Establishing acquisition standards to ensure functional, security and operational requirements to be accurately identified and clearly detailed in request-for-proposals.	**ADVANTAGES OF APPLICATION SOFTWARE: (Royal Challengers Quit League)** • Rapid implementation • Cost • Quality • Low risk **METHODS OF VALIDATING PROPOSAL** • Checklists • Point Scoring Analysis • Public Evaluation Reports • Benchmarking problem for vendor's proposal • Test problems	**Validation of Vendors' proposals: (Vice-Chairman Manages Company's Portfolio)** • Vendor Support • Compatibility with Existing Systems • Maintainability of the proposed system • Cost benefits of the proposed system • Performance rating of the proposed system in relation to its cost

STAGE – IV – Part 2: DEVELOPMENT (PROGRAMMING TECHNIQUES AND LANGUAGES) **Objective:** To convert the specification into a functioning system. **Activities:** Application programs are written, tested and documented, conduct system testing. **Document/Deliverable:** A fully functional and documented system.	**Characteristics Of A Good Coded Program:** • Reliability • Robustness • Accuracy • Efficiency • Usability • Readability	**Program Debugging** Debugging refers to correcting programming language syntax and diagnostic errors so that the program compiles cleanly. It consists of: • Inputting the source program to the compiler, • Letting the compiler find errors in the program, • Correcting lines of code that are erroneous, and • Resubmitting the corrected source program as input to the compiler.
STAGE – V: SYSTEM TESTING UNIT TESTING **Categories of tests that a programmer typically performs on a program unit:** • Functional Tests • Performance Tests • Stress Tests • Structural Tests • Parallel Tests	**TYPES OF UNIT TESTING** • **Static Analysis Testing:** - Desk Check - Structured walk-through - Code inspection • **Dynamic Analysis Testing:** - Black Box Testing - White Box Testing - Gray Box Testing	**INTEGRATION TESTING** • Bottom-up Integration • Top-down Integration • Regression Testing
SYSTEM TESTING • Recovery Testing • Security Testing • Stress or Volume Testing • Performance Testing	**FINAL ACCEPTANCE TESTING** • Quality Assurance Testing • User Acceptance Testing: - Alpha Testing - Beta Testing	

STAGE – VI: SYSTEM IMPLEMENTATION EQUIPMENT INSTALLATION • Site Preparation • Installation of New Hardware/Software • Equipment Checkout **TRAINING PERSONNEL** • System Operators Training • Users Training	**CONVERSION PROCEDURE:** **Activities for successful conversion: (Fifa Played in South Africa)** • File conversion • Procedure conversion • System conversion • Scheduling personnel and equipment • Alternative plans in case of equipment failure	**System Implementation Conversion Strategies:** • Direct Implementation/Abrupt change-over • Phased implementation • Pilot implementation • Parallel running implementation
STAGE VII – POST-IMPLEMENTATION REVIEW & MAINTENANCE • Development Evaluation • Operation Evaluation • Information Evaluation	**SYSTEM MAINTENANCE** • Scheduled maintenance • Rescue maintenance • Corrective maintenance • Adaptive maintenance • Perfective maintenance • Preventive maintenance	**OPERATION MANUALS** • A cover page, a title page and copyright page; • A preface and information on how to navigate the user guide; • A contents page; • A guide on how to use at least the main functions of the system; • A troubleshooting section; • A FAQ (Frequently Asked Questions); • Where to find further help, and contact details; • A glossary and an index.

---****---

NEED FOR CONTROL AND AUDIT OF INFORMATION SYSTEMS:

Factors influencing an organisation toward control and audit of computers and the impact of the information systems audit function on organisations are –

- Organisational Costs of Data Loss
- Incorrect Decision Making
- Costs of Computer Abuse
- Value of Computer Hardware, Software and Personnel
- High Costs of Computed Error
- Maintenance of Privacy
- Controlled evolution of computer use
- Information Systems Auditing
- Asset Safeguarding Objectives
- Data Integrity Objectives
- System Effectiveness Objectives
- System Efficiency Objectives

EFFECT OF COMPUTERS ON INTERNAL CONTROLS:

1. **Change in the type and nature of internal controls: (RAM'S Personal Assistant)**
   - Record keeping
   - Access to assets and records
   - Management supervision and review
   - Segregation of duties
   - Personnel
   - Authorisation procedures
2. **Internal controls used within an organisation comprise of the following five interrelated components:**
   - Control environment
   - Risk assessment
   - Control activities
   - Information & communication
   - Monitoring

EFFECT OF COMPUTERS ON AUDIT

1. **Changes to evidence collection: (DEVIL)**
   - Data retention and storage
   - Audit Evidence
   - Lack of Visible output
   - Lack of a visible audit trail
   - Absence of Input documents
   - Legal issues
2. **Changes to Evidence Evaluation**
   - System generated transactions
   - Systematic error

RESPONSIBILITY FOR CONTROLS

- Long-range planning
- Long range planning and IT department
- Short range planning or tactical planning
- Personnel management controls

THE IS AUDIT PROCESS

- Assessment of internal controls within the IS environment to assure validity, reliability and security information.
- Assessment of the efficiency and effectiveness of the IS environment in economic terms.

FUNCTIONS OF IS AUDITOR

- Inadequate information security
- Inefficient use of corporate resources, or poor governance
- Ineffective IT strategies, policies and practices
- IT-related frauds

<table>
<tr>
<td>CATEGORIES OF IS AUDITS
• Systems and Applications
• Information Processing Facilities
• Systems Development
• Management of IT and Enterprise Architecture
• Telecommunications, Intranets and Extranets</td>
<td>STEPS IN INFORMATION TECHNOLOGY AUDIT:
• Scoping and pre-audit survey
• Planning and preparation
• Fieldwork
• Analysis
• Reporting
• Closure</td>
<td>COST EFFECTIVENESS OF CONTROL PROCEDURES:
Implementing and operating controls in a system involves –
• Initial set up cost
• Executing cost
• Correction costs
• Failure cost
• Maintenance costs</td>
</tr>
<tr>
<td>INFORMATION SYSTEMS CONTROL TECHNIQUES: The basic purpose of information system controls in an organisation is to ensure that the business objectives are achieved and undesired risk events are prevented or detected and corrected.</td>
<td colspan="2">OBJECTIVE OF CONTROLS:
The objective of control is to reduce or if possible eliminate the causes of the exposure to potential loss. Some categories of exposures are:
• Errors or omissions
• Improper authorizations and improper accountability
• Inefficient activity
Some of the critical control considerations in a computerized environment are:
• Lack of management understanding of IS risks.
• Absence or inadequate IS control framework.
• Absence of or weak general controls and IS controls.
• Lack of awareness and knowledge of IS risks.
• Complexity of implementation of controls.
The control objectives serve two main purposes:
• Outline the policies of the organisation as laid down by the management.
• A benchmark for evaluating whether control objectives are met.</td>
</tr>
</table>

AUUDITOR'S CATEGORISATION OF CONTROLS: • Preventive Controls • Detective Control • Corrective Controls • Compensatory Controls	**Classification of controls based on the nature of such controls with regard to the nature of IS resources to which they are applied:** • Environmental Controls • Physical Access Controls • Logical Access Controls • IS Operational Controls • IS Management Controls • SDLC Controls	**Category of controls is based on their functional nature/Components of Internal Control:** • Internal Accounting Controls • Operational Controls • Administrative Controls
CONTROL TECHNIQUES: • Organisational Controls • Management Controls • Financial Control Techniques • Data Processing Environment Controls • Physical Access Controls • Logical Access Controls • SDLC (System Development Life Cycle) Controls • Business Continuity (BCP) Controls • Application Control Techniques	**ORGANISATIONAL CONTROLS** • Reporting responsibility and authority of each function, • Definition of responsibilities and objectives of each functions, • Policies and procedures, • Job descriptions, • Segregation of duties. **MANAGEMENT CONTROLS** • Responsibility • An official IT structure • An IT steering committee	**FINANCIAL CONTROL TECHNIQUES:** • Authorisation • Budgets • Cancellation of documents • Documentation • Dual control • Input/output verification • Safekeeping • Segregation of duties • Sequentially numbered documents • Supervisory review
AUDIT TRAILS – Objectives: (DR. Audit) • Detecting Unauthorised Access • Reconstructing Events • Personal Accountability	**USER CONTROLS** • Boundary Controls • Input Controls • Processing Controls • Output Controls • Database Controls	**USER CONTROLS: ERROR IDENTIFICATION, CORRECTION AND RECOVERY CONTROLS** **Boundary control techniques are:** • Cryptography • Passwords • Personal Identification Numbers (PIN) • Identification Cards

Input Controls: Factors affecting coding errors as follows: • Length of the code • Alphabetic numeric mix • Choice of characters • Mixing uppercase/lowercase fonts • Sequence of characters • Existence/Recovery Controls	**Processing Controls:** • Run-to-run totals • Reasonableness verification • Edit checks • Field initialization • Exception reports • Existence/Recovery Controls	**Output Controls** • Storage and logging of sensitive, critical forms • Logging of output program executions • Spooling/Queuing • Controls over printing • Report distribution and collection controls • Retention controls • Existence/Recovery Controls
Database Controls: **The update controls are:** • Sequence Check Transaction and Master Files • Ensure All Records on Files are processed • Process multiple transactions for a single record in the correct order • Maintain a suspense account	**Database Controls:** **The Report controls are:** • Standing Data • Print-Run-to Run control Totals • Print Suspense Account Entries • Existence/Recovery Controls	**SYSTEM DEVELOPMENT AND ACQUISITION CONTROLS:** • Strategic master plan • Project controls • Data processing schedule • System performance measurements • Post-implementation review
CONTROLS OVER THE SYSTEM DEVELOPMENT PHASES AND AUDITOR'S ROLE • Problem definition • Entry and feasibility assessment • Analysis of the existing system • Formulation of strategic requirements (system design) • Organisational and job design • Information processing systems design • Application software acquisition/selection process	**CONTROL OVER SYSTEM AND PROGRAM CHANGES:** • Management of the change process • Change management controls • System change controls • Program change controls • Authorisation controls • Documentation controls • Testing and quality controls	**MANAGEMENT OF THE CHANGE PROCESS** • Provide feedback to stakeholders • Prevents system disruptions • Accepted changeover to a new system • Helps users to adapt to new roles • Documentation and follow up on the recommended and implemented process changes • The proposed change need to be reviewed to identify potential conflicts with other systems.

QUALITY CONTROL • Establishment of a quality culture • Quality plans • Quality assurance responsibilities • Quality control practices • System development life cycle methodology • Program and system testing and documentation • Quality assurance reviews & reporting • Training and involvement of end-user and quality assurance personnel • Development of a quality assurance knowledge base • Benchmarking against industry norms	**QUALITY CONTROL** • Quality Reviews • Contract/Warrants • Service Level Agreements (SLA)	**CONTROLS OVER SYSTEM IMPLEMENTATION** • Procedures development • Conversion • User final acceptance testing: - Performance testing - Volume testing - Stress testing - Security testing - Clerical procedures checking - Back-up and recovery - Parallel operation
ACTIVITIES TO BE UNDERTAKEN IN PIR: • The main functionality of the operational system • System performance and operation • The development techniques and methodologies employed • Estimated time-scales and budgets • Changes to requirements • Set out findings, conclusions and recommendations in a report	**AUDITOR'S ROLE/CONTROL CONSIDERATIONS:** • Interview business users • Interview security, operations and maintenance staff • Determine whether the system's requirements have been met • Review system problem reports and change proposals • Confirm that adequate internal controls have been built into the system • Confirm that an adequate Service Level Agreement has been drawn up and implemented • Confirm that the system is being backed up in accordance with user requirements • Review the Business Case • Review trends in transaction throughput	**CONTROL OVER DATA INTEGRITY, PRIVACY AND SECURITY – INFORMATION CLASSIFICATION: (TCP/IP)** • Top Secret • Highly Confidential • Proprietary • Internal use only • Public Documents

DATA INTEGRITY: The primary objective of data integrity control techniques is to prevent, detect, and correct errors in transactions as they flow through the various stages of a specific data processing program. **(SID is on the POT)** • Source data control • Input validation routines • On-line Data Entry controls • Data Processing and storage controls • Output controls • Data Transmission controls	**DATA INTEGRITY POLICIES** • Virus-Signature Updating • Software Testing • Division of Environments • Version Zero Software • Offsite Backup Storage • Quarter-End and Year-End Backups • Disaster Recovery	**DATA SECURITY** Data security encompasses the protection of data against accidental or intentional disclosure to unauthorised persons as well as the prevention of unauthorised unauthorised modification and deletion of the data.
SECURITY CONCEPTS AND TECHNIQUES CRYPTOSYSTEMS A cryptosystem refers to a suite of algorithms needed to implement a particular form of encryption and decryption.	**DATA ENCRYPTION STANDARD (DES):** The DES is a cipher (a method for encrypting information) which has enjoyed widespread use internationally. It is a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.	**PUBLIC KEY INFRASTRUCTURE (PKI):** The system is based on public key cryptography in which each user has a key pair – a unique electronic value called a public key and a mathematically related private key. The public key is made available to those who need to verify the user's identity. The private key is used to create an electronic identifier caller a digital signature that uniquely identifies the holder of the private key and can only be authenticated with the corresponding public key.

FIREWALLS **Types of Firewalls: (A SIP)** • Application-Level Firewalls • Proxy Server Firewalls • Stateful Inspection Firewalls • Packet Filter Firewalls	**HACKING:** Ways in which a hacker can hack- • NetBIOS • ICMP 'Ping' (Internet Control Message Protocol) • FTP (File Transfer Protocol) • RPC statd • HTTP	**Virus:** A virus is a program (usually destructive) that attaches itself to a legitimate program to penetrate the operating system. **Anti-virus Software:** • Scanners • Active Monitor and Heuistic Scanner • Integrity Checkers
LOGICAL ACCESS CONTROLS • Logical access controls restrict users to authorised transactions and functions. • There are logical controls over network access. • There are controls implemented to protect the integrity of the application and the confidence of the public when the public accesses the system.	**LOGICAL ACCESS PATHS: (D BOOT)** • Dial-up Ports • Batch Job Processing • Online Terminals • Operator Console • Telecommunication Network	**LOGICAL ACCESS ISSUES AND EXPOSURES:** • Access control software • Application software • Data • Data dictionary/directory • Dial-up lines • Libraries • Logging files • Operator systems exists • Password library • Procedure libraries • Telecommunication lines • Temporary disk files

ISSUES AND REVELATIONS RELATED TO LOGICAL ACCESS: **1. Technical Exposures: (Worms Destroyed D Horse by Throwing Bombs)** • Worms • Data Diddling • Rounding Down • Trojan Horse • Salami Techniques • Bombs: Time Bomb & Logic Bomb	**2. Asynchronous Attacks: (Pig Ltd.)** • Piggybacking: • Data Leakage • Wire-Tapping • Denial of Service	**3. Computer Crime Exposures: (Free DISCS)** • Financial Loss • Legal Repercussions • Disclosure of Confidential, Sensitive or Embarrassing Information • Industrial Espionage/Blackmail • Sabotage • Loss of Credibility/Competitive Edge • Spoofing
LOGICAL ACCESS CONTROL ACROSS THE SYSTEM • **User access management** - User registration - Privilege management - User password management - Review of user access rights • **User responsibilities** - Password use - Unattended user equipment • **Network access control** - Policy on use of network services - Enforced path - Segregation of networks - Network connection and routing control - Security of network services	• **Operating system access control** - Automated terminal identification - Terminal log-on procedures - User identification & authentication - Password management system - Use of system utilities - Duress alarm to safeguard users - Terminal time out - Limitation of connection time • **Application and monitoring system access control** - Information access restriction - Sensitive system isolation - Event logging - Monitor system use - Clock synchronization • **Mobile computing** - Mobile computing	**ROLE OF AN IS AUDITOR IN EVALUATING LOGICAL ACCESS CONTROLS:** • Reviewing the relevant documents pertaining to logical facilities • The potential access paths into the system • Deficiencies or redundancies • To verify test controls over access paths to determine its effective functioning • Evaluate the access control mechanism, analyse the test results and verify whether the control objectives has been achieved • Compare security policies and practices of other organisations

PHYSICAL ACCESS CONTROLS: PHYSICAL ACCESS ISSUES AND EXPOSURES- • Abuse of data processing resources • Blackmail • Embezzlement • Damage, vandalism or theft to equipments or documents • Modification of semester equipment and information • Public disclosure of sensitive information • Unauthenticated entry	**ACCESS CONTROL MECHANISMS** • **Identification** – the users have to identify themselves, thereby indicating their intend to request the usage of system resources. • **Authentication** – the users must authenticate themselves and the mechanism must authenticate itself. • **Authorisation** – the users request for specific resources, their need for those resources and their areas of usage of these resources. - Ticket oriented approach - List-oriented approach	**PHYSICAL ACCESS CONTROLS** 1. Locks on Doors • Cipher locks • Bolting Door Locks • Electronic Door Locks • Biometric Door Locks 2. Physical identification medium Personal Identification Numbers (PIN) • Plastic Cards • Cryptographic Control • Identification Badges 3. Logging on utilities • Manual Logging • Electronic Logging 4. Other means of controlling Physical Access like: Video Cameras, Security Guards, Controlled Visitor Access, etc.
ROLE OF IS AUDITOR IN PHYSICAL ACCESS CONTROLS: • Risk assessment • Controls assessment • Planning for review of physical access controls • Testing of controls	**ENVIRONMENTAL CONTROLS: ENVIRONMENTAL ISSUES AND EXPOSURES:** • Fire • Natural disasters • Power spike • Air conditioning failure • Electrical shock • Equipment failure • Water damage/flooding • Bomb threat/attack	

CONTROLS FOR ENVIRONMENTAL EXPOSURES/AUDIT AND EVALUATION TECHNIQUES FOR ENVIRONMENTAL CONTROLS: • Hand-Held Fire Extinguishers • Manual Fire Alarms • Fire Suppression Systems: - Dry-Pipe sprinkling systems - Water based systems - Halon systems • Regular Inspection by Fire Department • Water Detectors • Smoke Detectors • Strategically Locating the Computer Room • Fireproof Walls, Floors and Ceilings surrounding the Computer Room • Electrical Surge Protectors • Uninterruptible Power Supply (UPS)/Generator • Power Leads from Two Substations • Emergency Power-Off Switch • Wiring Placed in Electrical Panels and Conduit • Prohibitions against Eating, Drinking and Smoking within the Information Processing Facility Documented and Tested Emergency Evacuation Plans		

---****---

INTRODUCTION TO BASICS OF TESTING (REASONS FOR TESTING):

It is a process used to identify the correctness, completeness and quality of developed computer software.

Testing is a scientific process performed to determine whether the controls ensure the system design effectiveness as well as the implemented system controls operational effectiveness.

Testing of Controls involves obtaining the population and conducting the compliance tests:

1. Substantive Testing
2. Compliance Testing

THE INFORMATION SYSTEM (IS) CONTROLS AUDIT INVOLVES THE FOLLOWING THREE PHASES:

- **Planning**
- **Testing**
- **Reporting**

AUDIT PLANNING:

- The auditor uses the concepts of **materiality** and **significance** to plan both **effective e** and **efficient** audit procedures.
- The auditor is not required to spend resources on items of little importance.
- Some areas of the IS controls audit are not material or significant, and therefore warrant no audit attention.
- Planning occurs throughout the audit as an iterative process.

AUDIT TESTING:

- If the end-user applications are producing valid and accurate information.
- Computer-assisted techniques could be used.
- The auditor should test the ability and extent of error detection, correction and prevention.
- The auditor should look for controls such as input balancing and record or hash totals.
- The intensity/extent of the testing should be related to the sensitivity/importance of the application.
- Testing should reveal any type of exposure of sensitive data.

MORE ON AUDIT TESTING:

- The auditor must test the critical controls, processes, and apparent exposures. It calls for validation in several ways as follows:
- Asking different personnel the same question.
- Asking the same question in different ways.
- Comparing checklist answers to work papers, programs, documentation and tests.
- Comparing checklist answers to observations.
- Conducting mini-studies of critical phases of the operation.

IS CONTROLS AUDIT PROCESS: The IS Control Audit process involves: • Understanding of an entity and its operations • Understanding of the structure of the entity's networks • Identifying key areas of audit interest • Assessing IS risk • Identifying critical control points • Understanding of IS controls	**If the IS Controls Audit is performed as part of a Financial Audit:** The auditor is to obtain an understanding of internal control over financial reporting sufficient to assessee the risk of material misstatement of the financial statements.	**If the IS Controls Audit is performed as part of a Performance Audit:** • The availability of evidence outside the information system to support the findings and conclusions. • The relationship of information systems controls to data reliability. • Assessing the effectiveness of information systems controls as an audit objective.
IDENTIFY KEY AREAS OF AUDIT INTEREST: The auditor should identify key areas of audit interest, which are those that are critical to achieving the audit objectives. For each key area of audit interest, the auditor should document: • The operational locations of each key system or file • Significant components of the associated hardware and software • Prior audit problems reported	**The auditor should include the following information in the documentation of their preliminary understanding of the design of IS controls:** • Identification of entitywide level controls • Identification of business process level controls for key applications • Management's plans and actions and milestones • Documented security plans • Documented risk assessments for relevant systems • Documented business continuity of operations plans and disaster recovery plans • Audit plan	**PERFORMING INFORMATION SYSTEM CONTROLS AUDIT TESTS:** • As audit evidence is obtained through performing control testing. • The auditor should periodically assess the audit evidence obtained to identify any revisions needed to the audit plan. • The auditor determines whether to perform tests of the operating effectiveness of such controls. • The auditor should determine whether it is possible and practicable to obtain sufficient, appropriate audit evidence.

The auditor identifies control techniques and determines the effectiveness of controls at each of the following levels: • Entity Wide or Component Level (General controls) • System Level (General controls) • Business Process Application Level (General Controls + Business) • Process Application Control	**TESTS OF GENERAL CONTROLS AT THE ENTITYWIDE AND SYSTEM LEVELS:** • Test general controls through a combination of procedures. • If general controls at the entitywide and system levels are not effectively designed and operating (i) determine extent of risks (ii) identify and test any manual controls • If manual controls do not achieve the control objectives, determine whether IS controls are designed to achieve the objectives. • If not, then the auditor should develop appropriate findings to improve internal control.	**TESTS OF GENERAAL CONTROLS AT THE BUSINESS PROCESS APPLICATION LEVEL:** • Evaluate and test the effectiveness of general controls for those applications within which business process application controls are to be tested. • They are referred to as Application Security (AS) controls. • If general controls are not operating effectively, business process application controls will be ineffective. • If financial or performance audit, the IS controls specialist should discuss the nature and extent of risks resulting from ineffective general controls.

TESTS OF BUSINESS PROCESS APPLICATION CONTROLS AND USER CONTROLS: • If IS controls are not likely to be effective, the auditor should obtain a sufficient understanding of control risks to: - identify the impact on the audit objectives - design audit procedures - develop appropriate findings. • Whether manual controls achieve the control objectives • The auditor should identify and evaluate any specific IS controls that are designed to achieve the control objectives.	**TEST EFFECTIVENESS OF INFORMATION SYSTEM CONTROLS:** • Conduct tests of relevant control techniques that are effective in design to determine their effectiveness. • To test IS controls on a tiered basis, starting with the general controls at the entitywide and system levels, then general controls at the business process application level, and concluding with tests at the business process application level. • Ineffective IS controls at each tier generally preclude effective controls at the subsequent tier. • Determine whether entitywide and system level general controls are effectively designed, implemented and operating effectively. • The auditor should conclude whether such controls are effectively designed and placed in operation.

TESTING CRITICAL CONTROL POINTS: • The auditor should evaluate the effectiveness of IS controls. • The auditor should evaluate all potential ways in which the critical point could be accessed. • This would include assessing controls related to the network, operating system, and infrastructure application components. • Determine the appropriate scope of audit: (a) the organisational entities to be addressed (b) the breadth of the audit (c) the types of IS controls to be tested.	**APPROPRIATENESS OF CONTROL TESTS:** • Inquiries of IT and management personnel • Questionnaires can be used • Observation of the operation of controls • Review documentation of control policies and procedures • Inspection of approval • Analysis of system information obtained through system or specialized software • Data review and analysis of the output of the application processing • Reperformance of the control	**Based on the results of controls tests, the auditor should determine whether the control techniques are operating effectively:** • Controls that are not operating effectively are potential IS control weaknesses. • For each potential weakness, there are specific compensating controls to mitigate the potential weakness. • If the auditor could adequately mitigate the potential weakness, he should obtain evidence. • If it effectively mitigates the potential weakness, conclude that the control activity is achieved. • If the potential weakness is not effectively mitigated, the potential weakness is an actual weakness.

DOCUMENTATION OF CONTROL TESTING PHASE: • An understanding of the information systems • IS Control objectives and activities • By level and system sublevel, a description of control techniques used by the entity • By level and sublevel, specific tests performed • Documentation that describes the nature, timing, and extent of the tests • Evidence of the effective operation of the control techniques • Conclusions about the effectiveness of the entity's IS controls	**AUDIT REPORTING:** • Audit Objectives • Report Audit Results • Substantive Testing • Documenting Results • Audit Finding • Analysis • RE-examination • Standards Compliance • Facts • Verification • Cause • Exposure and Materiality

CONCURRENT/CONTINUOUS AUDIT - Types of Audit Tools: (She Is Smart and Cool) • Snapshots • Integrated Test Facility (ITF) • System Control Audit Review File (SCARF): - Application system errors - Policy and procedural variances - System exception - Statistical sample - Snapshots and extended records - Performance measurement • Continuous and Intermittent Simulation (CIS)	**Advantages** • Timely, comprehensive and detailed auditing • Surprise test capability • Information to system staff on meeting of objectives • Training for new users	**Disadvantages** • Auditors should be able to obtain resources required from the organisation to support it. • More likely to be used if auditors are involved in the development work of a new application system. • Auditors need the knowledge and experience of working with computer systems to be able to use it effectively and efficiently. • It is more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high. • It won' be effective if the application system is not relatively stable.
REVIEW OF HARDWARE: • The capacity management procedures for hardware • The hardware acquisition plan • The change in management controls • The preventive maintenance practices	**OPERATING SYSTEM REVIEW:** • Interview technical and system programming manager • Review the feasibility study and selection process • Review cost/benefit analysis • Review controls over the installation • Review system software maintenance activities • Review system software change controls • Review systems documentation • Review software implementation	**REVIEWING THE NETWORK:** • LAN topology and network design • Significant LAN components • Network topology • LAN uses • LAN administrator • Significant groups of LAN users • Functions performed by the LAN Administrator • LAN transmission media and techniques, including bridges, routers and gateways

---****---

Risk: is the likelihood that an organisation would face a vulnerability being exploited or a threat becoming harmful. **Threat:** is any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data and denial of services.	**Vulnerability** is the weakness in the system safeguards that exposes the system to threats. **Exposure** is the extent of loss the organisation has to face when a risk materializes.	**Attack** is a set of actions designed to compromise confidentiality, integrity, availability or any other desired feature of an information system. **Residual Risk:** Any risk still remaining after the counter measures are analysed and implemented is called residual risk.
• **THREATS TO THE COMPUTERISED ENVIRONMENT: (The DEMAND Curve is Perfectly Fine)** • Theft or destruction of computing resources • Disgruntled Employees • Errors • Malicious Code • Abuse of access privileges by employees • Natural disasters • Downtime due to technology failure • Communication failure • Power Loss • Fire, etc.	**THREATS DUE TO CYBER CRIMES: (Due To Computer Virus Entire Fraud Slipped Off)** • Denial of service • Theft of proprietary information • Computer Virus • Embezzlement • Fraud • Sabotage or Vandalism • Other	**RISK MANAGEMENT PROCESS:** • Identify the risks • Assess the identified risk • Classify the risks • Identify various managerial actions that can reduce exposure • Look out for technological solutions • Identify the contribution of the technology in reducing the overall risk exposure. • Evaluate the technology risk premium and compare the same with the possible value of loss from the exposure. Match the analysis with the management policy

RISK MANAGEMENT: • **Systematic risks** • **Unsystematic risks**	**THE RISK MANAGEMENT CYCLE:** • Risk Identification • Risk Assessment • Risk Mitigation	
RISK IDENTIFICATION: • What is the probability that things can go wrong? **(Probability)** • What is the cost if what can go wrong does go wrong? **(Exposure)**	**The purpose of a risk evaluation is to:** • Identify the probabilities of failures and threats • Calculate the exposure, i.e. the damage or loss to assets • Make control recommendations keeping the cost-benefit analysis in mind	**TECHNIQUES FOR RISK EVALUATION:** • Judgement and intuition • The Delphi approach • Scoring • Quantitative Techniques
RISK ASSESSMENT: Risk assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster.	**Various areas to determine the risk:** **(Please Issue Anil Dhirubhai Ambani's ID)** • Prioritisation • Identifying critical applications • Assessing their impact on the organisation • Determining recovery time-frame • Assess Insurance coverage • Identification of exposures & implications • Development of recovery plan	**RISK MITIGATION:** Factor or casual analysis can help related characteristics of an event to the probability and severity of the operational losses. This will enable the organisation to decide whether or not to invest in information system or people (hazards) so events (frequency) or the effect of events (severity) can be minimized.
COMMON RISK MITIGATION TECHNIQUES • Insurance • Outsourcing • Service Level Agreements		

---****---

BUSINESS CONTINUITY PLANNING The business continuity plan is a guiding document that allows the management team to continue operations. It is a plan for running the business under stressful and time compressed situations.	**Business continuity plan covers:** Business resumption planning Disaster recovery planning Crisis recovery planning Crisis management	**The business continuity life:** Risk assessment Determination of recovery alternatives Recovery plan implementation Recovery plan validation
OBJECTIVES AND GOALS OF BUSINESS CONTINUITY PLANNING **The objectives:** • Provide for the safety of people on the premises at the time of disaster • Continue critical business operations • Minimise the duration of a serious disruption to operations and resources • Minimize immediate damage & losses • Establish management succession and emergency powers • Facilitate effective co-ordination of recovery tasks • Reduce the complexity of the recovery effort Identify critical lines of business and supporting functions	**The goals of the business continuity plan:** • Identify weaknesses and implement a disaster prevention program • Minimize the duration of a serious disruption to business operations • Facilitate effective co-ordination of recovery tasks • Reduce the complexity of the recovery effort	

DEVELOPING A BUSINESS CONTINUITY PLAN: • Providing an understanding of the efforts required to develop and maintain a recovery plan to the management • Obtaining commitment from management • Defining recovery requirements from the perspective of business functions • Documenting the impact of an extended loss to operations and key business functions • Focusing appropriately on disaster prevention and impact minimization • Selecting business continuity teams • Developing a business continuity plan • Defining integration into ongoing business planning and system development processes	**PHASES OF BUSINESS CONTINUITY PLANNING: (Pakistan Vs Bangladesh Delayed Playing Their Match In India)** • Pre-Planning Activities (Business continuity plan initiation) • Vulnerability Assessment and General Definition of Requirements • Business Impact Analysis • Detailed Definition of Requirements • Plan Development • Testing Program • Maintenance Program • Initial Plan Testing and Plan Implementation	**THREATS AND RISK MANAGEMENT: (Uncle Charlie HIDES)** • Unauthorised users attempt to gain access to the system and system resources • Lack of Confidentiality • Hackers and computer crimes • Lack of Integrity • Disgruntled employees • Terrorism and Industrial Espionage • Lack of System Availability
TYPES OF PLANS: **(Boys Entered the Room)** • Back-up Plan • Emergency Plan • Recovery Plan	**SOFTWARE AND DATA BACK-UP TECHNIQUES: TYPES OF BACK-UPS: (I Managed to Draw a Flower)** • Incremental Backup • Mirror Backup • Differential Backup • Full Backup	**ALTERNATE PROCESSING FACILITY ARRANGEMENTS:** • Cold site • Hot site • Warm site • Reciprocal agreement

BACK-UP REDUNDANCY: **(Where is MOM)** • Where to Keep the Backups • Multiple Backup Media • Off-Site Backup • Media – Rotation – Tactics	**TYPES OF BACK-UP MEDIA:** • Floppy Diskettes • Compact Disks • Tape Drives • Disk Drives • Removable Disks • DAT (Digital Audio Tape) drives • Optical Jukeboxes • Autoloader Tape Systems • USB Flash Drive • Zip Drive	**DISASTER RECOVERY PROCEDURAL PLAN:** • The conditions for activating the plans • Emergency procedures • Fallback procedures • Resumption procedures • A maintenance schedule • Awareness and education activities • The responsibilities of individuals • Contingency plan • The purpose and scope of the plan • Contingency plan testing and recovery procedure • List of phone numbers of employees • Emergency phone list for fire, police, back-up location, etc. • Medical procedure to be followed • Insurance papers and claim forms • Names of employees trained for emergency situation, first aid and life saving techniques
TESTING METHODOLOGY AND CHECKLIST: **(High Court Meeting on Friday)** • Hypothetical • Component • Module • Full	**AUDIT TOOLS AND TECHNIQUES:** **(I-PAD)** • Internal Control Auditing • Penetration Testing • Automated Tools • Disaster and Security Checklists	

---****---

ERP:

- An ERP system is a fully integrated business management system – covering functional areas of an enterprise
- It organizes and integrates – operation processes and information flows, to make optimum use of resources such as men, material, money and machine
- ERP aims at one database, one application, and one user interface for the entire enterprise.

WHY COMPANIES UNDERTAKE ERP: (My House Is Completely Furnished)

- Standardise and speed up Manufacturing processes
- Standardise HR information
- Reduce Inventory
- Integrate Customer order information
- Integrate Financial Information

ERP CHARACTERISTICS: (Mein hoon Characteristics of erp, Promise karta hoon, Beyond the company jhake, Flexible ho kar, New Technology launga)

- Modular & Open
- Comprehensive
- Best Business Practices
- Beyond The Company
- Flexibility
- New Technologies

BENEFITS OF ERP

- Increased control of invoicing and payment processing
- Reduce paper documents
- Improves timeliness of information
- Greater accuracy of information
- Faster response and follow-up on customers
- More efficient cash collection
- Better monitoring and quicker resolution of queries
- Helps to achieve competitive advantage by improving its business process
- Provides a unified customer database usable by all applications

FEATURES OF ERP:

- ERP provides multi-functions
- Functions are effectively integrated and information is immediately updated upon entry of any information.
- Has end to end Supply Chain Management
- ERP facilitates company-wide Integrated Information System covering all functional areas
- ERP performs core activities and increases customer service, thereby augmenting the corporate image.
- ERP bridges the information gap across organisations.
- ERP provides complete integration of systems not only across departments but also across companies under the same management.
- ERP is the solution for better project management.
- ERP allows automatic introduction of the latest technologies
- ERP eliminates most business problems
- ERP provides intelligent business tools

<table>
<tr>
<td>BUSINESS PROCESS REENGINEERING (BPR):
Fundamental rethinking [Eliminating processes not adding value to customers – “Why do you do what you do”]
&
Radical redesign [Reinventing and not enhancing or improving – “Whatever was being done in past, it was all wrong”- Do not get biased by it.]
=
Of processes to achieve dramatic improvement in critical, contemporary measure of performance such as cost, quality, etc. [Major transformation (80 – 90% growth story)]</td>
<td>BUSINESS ENGINEERING: Business Engineering = Business Process Reengineering + Information Technology</td>
<td>KEY PLANNING AND IMPLEMENTATION DECISIONS:
• ERP or Not to ERP?
• Follow Software’s Processes or Customize?
• In-house or Outsource?
• “Big Bang”or Phased Implementation?</td>
</tr>
<tr>
<td>ERP IMPLEMENTATION METHODOLOGY:
• Identifying the needs
• Evaluating the ‘As Is’ situation
• Deciding the ‘Would be’ situation
• Reengineering the Business Process
• Evaluating the various available ERP
• Finalizing of the most suitable ERP
• Installing the required hardware
• Finalizing the implementation consultants
• Implementation</td>
<td colspan="2">IMPLEMENTTION GUIDELINES FOR ERP:
• Understanding the corporate needs and culture of the organisation
• Doing a business process redesign exercise prior to starting the implementation
• Establishing a good communication network across the organisation
• Providing a strong and effective leadership
• Finding an efficient and capable project manager
• Creating a balanced team of implementation consultants
• Selecting a good implementation methodology with minimum customisation
• Training end users
Adapting the new system and making the required changes in the working environment to make effective use of the system in future</td>
</tr>
</table>

POST-IMPLEMENTATION:

Popular expectations are:

- An improvement in processes
- Increased productivity on all fronts
- Total automation and disbanding of all manual processes
- Improvement of all key performance indicators
- Elimination of all manual record keeping
- Real time information system available to concerned people on a need basis
- Total integration of all operations

Some of the fears on ERP implementations are:

- Job redundancy.
- Loss of importance as information is no longer an individual prerogative.
- Change in job profile:
- An organisational fear of loss of proper control and authorisation.
- Increased stress caused by greater transparency.
- Individual fear of loss of authority.

The ground realities are:

- Changing the organisation involves three levels-strategies, business process and change, and consequential organisation change.
- Measuring key performance indicators brings in new culture.
- The genetic nature of the ERP packages is such that there would be processes peculiar to some sectors and organisations, which may have to be kept out of the process.
- Some of the processes are better done manually.

RISK AND GOVERNANCE ISSUES IN ERP:

(<u>S</u>he <u>B</u>ought a <u>C</u>rate of <u>SODA</u>, <u>ID</u> & <u>DSP</u>)

- <u>S</u>ingle point of failure
- <u>B</u>road system access
- <u>C</u>hange management
- <u>S</u>tructural changes
- <u>O</u>nline, real-time
- <u>D</u>istributed computing experience
- <u>A</u>udit expertise
- <u>J</u>ob role changes
- <u>D</u>ependency on external assistance
- Program interfaces and <u>D</u>ata conversions
- <u>D</u>ata content quality
- <u>S</u>ingle sign on
- Privacy and confidentiality

SAMPLE LIST OF ERP VENDORS:

- Baan (The Baan Company)
- Oracle Applications (Oracle)
- Prism (Marcam Corporation)
- R/3 (SAP)
- System 21 (JBA)

---****---

AAS 29: requires the auditor to consider the effect of a CIS environment on his audit and discuss the risk and caution that an auditor should exercise while carrying out traditional audit objectives in a computer information system environment and elaborates on the following:

- The auditor's responsibility in gaining sufficient understanding and assurance on the adequacy of accounting and internal controls.
- The potential impact of auditing in a CIS on the assessment of control and audit risks.
- The auditor is required to determine the following factors to determine the effect of CIS environment on the audit arising from.
- The extent to which the CIS is used for recording, compiling and analysing accounting information.
- The system of internal controls relating to the authorised, complete, accurate and valid processing & reporting procedures.
- The impact of CIS accounting system on the audit trail.

BS 7799: is an International Standard (British Standard) setting out the requirements for an Information Security Management System.

- It helps identify, manage and minimize the range of threats to which information is regularly subjected.
- The "Security Code of Conduct" was a originator from which grew BS 7799, which has, in turn, subsequently grown into ISO 17799.
- BS 7799 was originally just a single standard, and had the status of a Code of Practice. In other words, it provided guidance for organisations, but hadn't been written as specification that could form the basis of an external third party verification and certification scheme.

Objectives: (CIA)

BS 7799 focused on protecting the **Confidentiality, Integrity and Availability** of organisational information.

BENEFIS OF USING BS 7799

- Reduced operational risk
- Increased business efficiency
- Assurance that information security is being rationally applied

This is achieved by ensuring that:

- Security controls are justified.
- Policies and procedures are appropriate.
- Security awareness is god amongst staff and managers.
- All security relevant information processing and supporting activities are auditable and are being audited.
- Internal audit, incident reporting/management mechanisms are being treated appropriately.
- Management actively focus on information security and its effectiveness.

COMPONENTS OF BS 7799:

- BS 7799 (ISO 17799) Part 1 – Code of Practice on Information Security Management
- BS 7799 Part 2 – Specification for Information Security Management Systems

ISO 27001 – (BS 7799: PART II) – INFORMATION SECURITY MANAGEMENT STANDARD (ISMS): To address assets to be protected, organisation approach to risk management, control objectives and control, and degree of assurance required. • Establishing Management Framework • Implementation • Documentation	**AREAS OF FOCUS OF ISMS: (SOAP's Physics & Chemistry Allows Scientists to Build Cinthol)** • Security Policy • Organisational Security • Asset Classification and Control • Personnel Security • Physical and Environmental Security • Communications and Operations Management • Access Control • Systems Development and Maintenance • Business Continuity Management • Compliance	**CMM – CAPABILITY MATURITY MODEL:** The CMM presents sets of recommended practices in a number of key process areas that have been shown to enhance software process capability. The CMM was designed to guide software organisations in selecting process improvement strategies by determining current process maturity and identifying the few issues most critical to software quality and process improvement.
THE FIVE LEVELS OF SOFTWARE PROCESS MATURITY: (I Remember Designing My Office) • Level 1 – The Initial Level • Level 2 – The Repeatable Level • Level 3 – The Defined Level • Level 4 – The Managed Level • Level 5 - The Optimizing Level	**CONTROL OBJECTIVES FOR INFORMATION RELATED TECHNOLOGY (COBIT):** The ISACF developed COBIT. COBIT is a trademark of generally applicable information systems security and control practices for IT controls. COBIT, which consolidates standards from 36 different sources into a single framework, is having a big impact on the information systems profession.	**The COBIT framework allows:** • Management to benchmark the security and control, practices of IT environments. • Users of IT services to be assured that adequate security and control exist • Auditors to substantiate their opinions on internal control and to advice on IT security and control matters.

The COBIT framework addresses the issue of control from three vantage points or dimensions: • Business Objectives • IT resources • IT processes	**COBIT – IT GOVERNANCE MODEL:** • Quality requirements • Fiduciary requirements • Security requirements	**BUSINESS OBJECTIVES/COBIT'S WORKING DEFINITIONS: (CIA & Cops Eat Eggs Regularly)** • Confidentiality • Integrity • Availability • Compliance • Effectiveness • Efficiency • Reliability of Information
IT RESOURCES: **(DID Tendulkar Pay A Fine)** • Data • Technology • People • Application systems • Facilities	**IT PROCESSES/THE COBIT FRAMEWORK/DOMAIN OF COBIT:** **(My Dad Is Powerful)** • Monitoring • Delivery and Support • Acquisition and Implementation • Planning and Organisation	**COBIT AND OTHER STANDARDS:** • COBIT and ISO 17799 (BS 7799) • COBIT and Sarbanes Oxley • COSO and COBIT
COCO: The "Guidance on Control" report, known colloquially as CoCo, was produced by The Canadian Institute of Chartered Accountants. CoCo does not cover any aspect of information assurance per se. It is concerned with control in general. CoCo can be said to be a concise superset of COSO.	**It use the same three categories of objectives:** **(Cops Eat Eggs Regularly)** • Compliance with applicable laws and regulations • Effectiveness of operations • Efficiency of operations • Reliability of financial reporting	**Concepts about "control":** • Control is affected by people throughout the organisation • People who are accountable for achieving objectives should also be accountable for the effectiveness of control • Organisations are constantly interacting and adapting • Control can be expected to provide only reasonable assurance, not absolute assurance

<table>
<tr><td>ITIL (IT INFRASTRUCTURE LIBRARY):
The IT Infrastructure Library (ITIL) is so named as it originated as a collection of books (standards) each covering a specific ‘practice’ within IT management.</td><td colspan="2"><u>The eight ITIL books and their disciplines are:</u>
The IT Service Management sets relating to:
1. Service Delivery
2. Service Support
Other operational guidance relating to:
3. ICT Infrastructure Management
4. Security Management
5. The Business Perspective
6. Application Management
7. Software Asset Management
8. Planning to Implement Service Management</td></tr>
<tr><td>SYSTRUST AND WEBTRUST:
• SysTrust engagements are designed for the provision or advisory services or assurance on the reliability of a system
• WebTrust engagements relate to assurance or advisory services on an organisation’s system related to e-commerce</td><td><u>Principles and Criteria:</u> (SAP CO.)
• <u>S</u>ecurity
• <u>A</u>vailability
• <u>P</u>rocessing integrity
• <u>C</u>onfidentiality
• <u>O</u>nline privacy</td><td><u>Broad Areas:</u> (Policies Communicates Procedures and also Monitors it)
• <u>P</u>olicies
• <u>C</u>ommunications
• <u>P</u>rocedures
• <u>M</u>onitoring</td></tr>
<tr><td>HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) were enacted by the U.S. Congress for:
• Protection of health insurance coverage for workers and their families when they change or lose their jobs
• Administrative Simplification provisions</td><td>SAS 70 – STATEMENT OF AUDITING STANDARDS FOR SERVICE ORGANISATIONS: A SAS 70 audit or service auditor’s examination is widely recognized, because it represents that a service organisation has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes.</td><td>SERVICE AUDITOR’S REPORTS:
• Type I report
• Type II report</td></tr>
</table>

---**---**

WHAT INFORMATION IS SENSITIVE: • Strategic Plans • Business Operations • Finances	**WHAT STEPS ARE NEEDED TO TAKE TO KEEP CRITICAL INFORMATION PROTECTED:** • Not all data has the same value • Know where the critical data resides • Develop an access control methodology • Protect information stored on media • Review hardcopy output	**PROTECTING COMPUTER-HELD INFORMATION SYSTEMS:** • Need to know what the information systems are and where these are located. • Need know the value of the information held and how difficult it would be to recreate if it were damaged or lost. • Need to know who is authorised to access the information and what they are permitted to do with the information. • Need to know how quickly information needs to be made available should it become unavailable for whatever reason
TYPES OF PROTECTION THAT AN ORGANISATION CAN USE: 4. Preventative Information Protection • Physical • Logical (Technical) • Administrative 5. Restorative Information Protection 6. Holistic Protection	**INFORMATION SECURITY POLICY:** A Policy is a plan or course of action, designed to influence and determine decisions, actions and other matters. The security policy is a set of laws, rules, and practices that regulates how assets including sensitive information are managed, protected, and distributed within the user organisation.	**ISSUES TO ADDRESS:** • A definition of information security • Reasons why information security is important to the organisation, and its goals and principles • A brief explanation of the security policies, principles, standards and compliance requirements • Definition of all relevant information security responsibilities • Reference to supporting documentation

TYPES OF INFORMATION SECURITY POLICIES AND THEIR HIERARCHY: (U And I Can Obviously Nail It)

- User Security Policy
- Acceptable Usage Policy
- Information Security Policy
- Conditions of Connection
- Organisational Information Security Policy
- Network & System Security Policy
- Information Classification Policy

COMPONENTS OF THE SECURITY POLICY:

- Purpose and Scope of the Document and the intended audience
- The Security Infrastructure
- Security policy document maintenance and compliance requirements
- Incident response mechanism and incident reporting
- Security organisation structure
- Inventory and Classification of assets
- Description of technologies and computing structure
- Physical and Environmental Security
- Identify Management and access control
- IT Operations management
- IT Communications
- System Development and Maintenance Controls
- Business Continuity Planning
- Legal Compliances
- Monitoring and Auditing Requirements
- Underlying Technical Policy

PURPOSE OF THE AUDIT POLICY:

To provide the guidelines to the audit team to conduct an audit on IT based infrastructure system. Common security threats are:

- Access to confidential data
- Unauthorised access of the computers
- Password disclosure compromise
- Virus infections
- Open ports, which may be accessed from outsiders
- Unrestricted modems unnecessarily open ports

Objective and the scope of the IS Audit policy:

- Safeguarding of Information System Assets/Resources
- Maintenance of Data Integrity
- Maintenance of System Effectiveness
- Ensuring System Efficiency
- Compliance with Information System related policies, guidelines, circulars, and any other instructions requiring compliance in whatever name called.

SCOPE OF IS AUDIT: The scope of information system auditing should encompass the examination and evaluation of the adequacy and effectiveness of the system of internal control and the quality of performance by the information system. The scope of the audit will also include the internal control system(s) for the use and protection of information and the information system, as under: **(Did Tendulkar Pay A Fine)** • Data • Technology • People • Application systems • Facilities	**AUDIT WORKING PAPERS AND DOCUMENTATION:** • The nature of the engagement • The form of the auditor's report • The nature and complexity of client's business • The nature and condition of client's records and degree of reliance on internal controls • The permanent audit file • The current file	**IS AUDIT REPORTS:** **(Can Tina Sit Front Of Anil?)** 1. Covered and Title Page 2. Table of Contents 3. Summary/Executive Summary 4. Introduction • Context • Purpose • Scope • Methodology 5. Findings 6. Opinion 7. Appendices

---****---